Fall 2007
Volume 9
Number 2

The Guardian

The Source for Antiterrorism Information

In This Issue

A Joint Staff, Deputy Directorate for Antiterrorism/Homeland Defense, Antiterrorism/Force Protection Division Publication

The Pentagon, Room MB917
Washington, DC 20318

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Guardian. Volume 9, Number 2, Fall 2007	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Deputy Directorate for Antiterrorism/Homeland Defense,Antiterrorism/Force Protection Division,The Pentagon, Room MB917,Washington,DC,20318**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**43**	

"Nearly six years after the 9/11 attacks, America remains a nation at war. The terrorist network that attacked us that day is determined to strike our country again, and we must do everything in our power to stop them. A key lesson of September 11 is that the best way to protect America is to go on the offense, to fight the terrorists overseas so we don't have to face them here at home. And that is exactly what our men and women in uniform are doing across the world.

The key theater in this global war is Iraq. Our troops are serving bravely in that country. They're opposing ruthless enemies, and no enemy is more ruthless in Iraq than al Qaeda. They send suicide bombers into crowded markets; they behead innocent captives and they murder American troops. They want to bring down Iraq's democracy so they can use that nation as a terrorist safe haven for attacks against our country. So our troops are standing strong with nearly 12 million Iraqis who voted for a future of peace, and they do so for the security of Iraq and the safety of American citizens."

— President George W. Bush
24 July 2007

"Violent extremist networks and ideologies will continue be a threat to the United States and our allies for many years …The ambition of these networks to acquire chemical, biological, and nuclear materials is real, as is their desire to launch more attacks on our country and our interests around the world."

— Secretary of Defense Robert Gates
26 April 2007

"Our terrorist adversaries have declared war, openly and explicitly, against the United States, our friends and allies, and all who love freedom and liberty. They are ruthless, and they are patient … and no nation or part of the world is immune. All who love liberty and freedom are fair game for them, and the conflict is likely to be a long one … This is not the time for America to pull back from the world. The greater the freedom enjoyed by other countries, the more secure our own nation, and the world, will be. This is a time for America's bold leadership—and for international cooperation and resolve."

— Deputy Secretary of Defense Gordon England
24 May 2007

Last issue, I posed the question on whether it is time for *The Guardian* to change formats. As DOD becomes committed to an all-hazards approach to force protection, this magazine will change as well. Past articles on pandemic influenza and a current article about counter-intelligence highlight this change. Your submissions detailing this approach, as well as the traditional force protection issues, are strongly encouraged and always welcome.

The Deputy Directorate for Antiterrorism and Homeland Defense continues to work hard to protect our Soldiers, Sailors, Airmen, and Marines from the dangers of terror attacks. We also endeavor to maximize the military response to a domestic Chemical, Biological, Radiation, Nuclear, or high-yield Explosive (CBRNE) attack. Yet, the National Combating Weapons of Mass Destruction (CWMD) strategy has several gaps, seams, and shortfalls. Specifically, current DOD DOTMLPF for Consequence Management (CM) needs additional emphasis. Unless the Department makes a major shift in policy direction, we may not be prepared to meet our national requirements in a crisis. The Joint Staff is also dedicated to providing immediate assistance to victims of natural disasters, such as hurricanes and earthquakes. As you can see, the DOD does not just focus on Iraq and Afghanistan, but also on protecting our citizens at home and abroad and planning for all contingencies to ensure a rapid, effective response to save lives and protect property.

Our forces engaging the enemy in Iraq and Afghanistan continue to be assaulted by insurgents and jihadists. In the midst of establishing better governance for Iraqis and Afghanis, our efforts are distracted by IEDs, sniper fire, and indirect fire from those who seek to thwart our success. We hope the ideas and material solutions presented in this magazine and others gain traction, or at least foster debate, to best protect our troops.

I encourage all of you to broaden your knowledge base concerning the terrorist threat. There are many good books, such as *The Looming Tower* and *A Peace to End All Peace,* detailing al Qaeda, Islamic extremism, and insurgencies, to name a few good topics. The United States has been involved in the Middle East since the birth of our nation with our conflict with the Barbary Pirates. Our strategic interests continue to lie in that region, and a better educated military can help to provide a better strategy to reach our desired end state.

To effect a broader Middle East peace, DOD's achievement in the Global War on Terror must realize successes against both Islamic extremist insurgencies and horrific terror attacks. As we approach the sixth observance of September 11, we must take pride in our successes without becoming complacent and recommit to learning the lessons from our failures.

"The price of freedom is eternal vigilance." —Thomas Jefferson

Peter M. Aylward
Brigadier General, US Army
J-3, Deputy Director for Antiterrorism/Homeland Defense

The Guardian newsletter is published for the Chairman of the Joint Chiefs of Staff by the Antiterrorism/Force Protection Division of the J3 Deputy Directorate for Antiterrorism/ Homeland Defense to share knowledge, support discussion, and impart lessons and information in an expeditious and timely manner. *The Guardian* is not a doctrinal product and is not intended to serve as a program guide for the conduct of operations and training. The information and lessons herein are solely the perceptions of those individuals involved in military exercises, activities, and real-world events and are not necessarily approved as tactics, techniques, and procedures.

SUBMITTING NEWS & ARTICLES

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Joint Staff, DOD, or any other agency of the Federal Government. The editors invite articles and other contributions on antiterrorism and force protection of interest to the Armed Forces. Local reproduction of our newsletter is authorized and encouraged.

Entry Control Point (ECP) Pilot Program

By Kelly Rose, ManTech SETA

The Technical Support Working Group (TSWG) is the US national forum that identifies, prioritizes, and coordinates interagency and international research and development (R&D) requirements for combating terrorism. TSWG rapidly develops technologies and equipment to meet the high-priority needs of the antiterrorism community and addresses joint international operational requirements through cooperative R&D with major allies.

Since 1986, TSWG has pursued technologies for combating terrorism in the broad context of national security by providing a cohesive interagency forum to define user-based technical requirements spanning the federal interagency community. By harnessing the creative spirit of US and foreign industry, academic institutions, government, and private laboratories, TSWG ensures a robust forum for technical solutions to the most pressing counterterrorism requirements.

Strategic Concept for Entry Control Operations

Lessons learned during Operation ENDURING FREEDOM and Operation IRAQI FREEDOM reveal that coalition forces operating in and around forward operating bases (FOB) within the United States Central Command (CENTCOM) area of responsibility (AOR) confront an increased threat from terrorists.

Insurgents predominantly attack in identifiable styles: multiple attacks and complex attacks, with active experimentation. Multiple attacks consist of simultaneous attacks, similar to the London attacks in 2005. In many cases in theater, the "double-tap" tactic is used, in which one truck rams a vehicle barrier and explodes, causing damage and opening a lane for a second vehicle to drive into the compound and detonate. Complex attacks, such as the attack on the Syrian Embassy in September 2006, use any combination of suicide bombers, vehicle-borne improvised explosive devices (VBIED), and direct or indirect fire, creating diversions. Finally, insurgents and terrorists use active experimentation as a means to probe the defenses of US and coalition forces in order to see who responds and how forces react to incidents.

Force protection issues should be addressed in the master plan of any secure facility in order to provide sufficient protection of critical facility personnel and assets. Improvised explosive devices (IED), VBIEDs, and suicide bombers pose increased threats to both US forces and Iraqi security forces. As a result, it is necessary to construct hardened entry control points (ECP) with enhanced capabilities such as early warning systems, prescreening for suicide bombers, remote vehicle inspection, remote pedestrian inspection, and blast mitigation buildings and materials throughout.

The ECP Pilot Program, funded and managed by TSWG in cooperation with US Marine Corps Central Command, aims to use such capabilities to detect, prevent, and mitigate ECP attacks while providing increased force protection. The enhanced ECP design is an R&D effort, based on guidelines in the *Joint Forward Operating Base Force Protection Handbook*.[1]

ECPs under construction within the CENTCOM AOR will separate high- and low-risk vehicles and pedestrians and provide remote identification and search corridors for each.

Enhanced ECP Design

Early Warning Standoff Detection

Standoff detection is a vital component of a cohesive and layered approach to force protection. The earlier that threats can be detected, the greater the opportunities to protect personnel and assets. ECP standoff detection gives security forces an advantage: In addition to advanced warning of intruders, ECP perimeter security controls the pedestrian and vehicle flow, channeling pedestrians into different search corridors based on possible threat.

In the ECP Pilot Program, overwatch towers and intrusion detection systems will monitor identifiable threats at a standoff distance as well as ongoing ECP activities. Towers and adjoining shelters, constructed of hardened materials capable of absorbing and dissipating blast wave energy, will protect security forces in the event an explosive detonates. The overwatch towers will also incorporate remote weapon systems, allowing security forces to defend the ECP without being subject to return fire.

Vehicle barriers surrounding the ECP will prevent observation of and access to restricted ECP areas. Barriers will also serve to expedite control of pedestrian and vehicle entry and exit, define perimeters, establish deterrents to attackers, and channel the flow of pedestrian and vehicle traffic through designated areas.

ECP Pilot Program technologies may include Metalith™ perimeter security barriers, the Dynatower and Dynablok™ blast mitigation system, the SPIDER stabilized automatic intruder detection system, and the Telepresent Rapid Aiming Platform (TRAP).

ENHANCED ECP TECHNOLOGY

Some specific technology products have been selected by TSWG for potential implementation in the ECP Pilot Program. Comparable products may meet operational requirements.

SPIDER

Spider

The SPIDER stabilized automatic intruder detection system combines motion detection with an assessment imaging system. The early warning system uses a 360° panoramic view camera with pan, tilt, and zoom capabilities. SPIDER detects intruders at ranges greater than 5 km and provides visual and audible alerts to security forces, which enables them to assess hostile intent.

> http://www.controp.co.il/PRODUCTS/IDSproducts/Products-IDS-Spider.asp/

DYNABLOK™ AND DYNATOWER

Dynablok™ wall in front of Dynatower

The Dynablok™ system was developed as an alternative blast mitigation method. It is capable of withstanding significant blast loads exceeding two to three times that of normal retrofits. The unique composition of Dynablok™ allows the energy of blast waves to be more easily absorbed and dissipated through the composite material, causing less damage to the structural integrity and eliminating spalling. This product is ideal for entry control points or perimeter sentry posts, overhead protection, and buildings without adequate standoff in high-threat locations.

Dynatower is an alternative structure aimed at reducing the threat from spalling or for use in conjunction with a Dynablok™ blast shield wall. Dynatower is marketed for its versatile use as an observation tower or vehicle check point in conjunction with an ECP. Dynatower is constructed of steel-reinforced, blast-tested concrete, making it more durable than regular concrete. The tower can be constructed in multiple heights depending on need. The turret is made of steel with ballistic and blast-proof shuttered window systems. Dynatower can be constructed on site within eight hours.

Dynatower and Dynablok are marketed as part of Dynasystems, under Explora Securities Ltd.

> http://www.dynablok.net/
> http://www.dynasystems.co.uk/

Dynatower

TRAP

Trap System

The Telepresent Rapid Aiming Platform (TRAP) is a highly accurate, remotely operated weapon system that provides security force personnel with the ability to fully function out of the line of fire, remain immune to hostile suppressive fire, and achieve the full accuracy of the weapon. TRAP supports multiple weapons systems, including 5.56 mm, 7.62 mm, and .50 caliber.

> http://precisionremotes.com/

METALITH BARRIERS

Metalith™ barrier testing

Infrastructure Defense Technologies' Metalith™ barriers are modular steel walls constructed from both 16- and 18-gauge corrugated steel panels that provide anti-ram vehicle protection as well as explosive mitigation. The barriers are shipped as prefabricated units and filled with soil or other indigenous material. The soil increases the barrier density, thus mitigating the energy of the vehicle as it slams into the barriers. The barriers also withstand harsh climates, making them cost-effective.

> http://www.themetalith.com/

Z BACKSCATTER VAN

Commercial ZBV

American Science & Engineering Inc.'s Z Backscatter Van (ZBV) employs backscatter X-ray technology, which detects low-density organic materials in complex, high-density backgrounds. This technology enables the operator to identify organic materials, including explosives and narcotics, which are depicted in the image as bright white objects.

The ZBV can be operated in stationary mode at entry points and checkpoints by parking the system and scanning vehicles as they drive past. The system can be remotely operated from a distance of up to 500 meters when parked. The most convenient aspect of the ZBV is that it can also operate in drive-by mode, scanning stationary objects or other moving vehicles. A stationary ZBV can be used in conjunction with the forward-scatter detection capability, which is used to highlight metallic objects such as hidden ordnance and weapons.

> http://www.as-e.com/products_solutions/zbv.asp/

Remote Vehicle Inspection

Prescreening systems in theater enable rapid screening of vehicles at inspection stations and checkpoints to determine the possible presence of many types of explosives, weapons, contraband, and even (concealed) people. The ability to effectively identify potential threats in vehicles or cargo still relies primarily on the operator; however, manual screening of large vehicles for the presence of explosives and other threats leaves the operator vulnerable to attack during inspection.

Automating the inspection tasks with advanced standoff technology will enable forces to remotely scan vehicles and identify threats. New advances in technology enhance the operator's ability to use and manipulate systems with respect to the particular threat environment, greatly influencing system effectiveness. It is expected that with multiple screening systems available for the ECP Pilot Program, properly trained security personnel will have the best possible detection tools and techniques.

Vehicle barriers will be used to control vehicle speed and guide drivers to the inspection site, which can include under-vehicle screening and cargo inspection systems. Vehicle occupants will be directed to the pedestrian inspection station for individual screening.

ECP Pilot Program technologies for pedestrian inspection may include Metalith™ barriers, the Z Backscatter Van (ZBV) mobile screening system with the forward-scatter detection (FSD) option, and the Gatekeeper under-vehicle inspection system.

Remote Pedestrian Inspection

Pedestrian inspection systems are used at ECPs to identify individuals entering a secure location and detect potential contraband and concealed explosives. Although pedestrians are prescreened with standoff detection, each person and his or her bags will undergo further screening to ensure no threats are present. This screening will be conducted within a hardened structure capable of absorbing and dissipating the energy of blast waves to ensure security forces are protected in the event that a suicide bomber or explosive detonates. Automated inspection systems offer the advantage of remote operation and improved detection capability, thereby reducing risk to security forces.

ECP Pilot Program technologies for pedestrian inspection may include Dynablok™, the Rapiscan Secure 1000 personnel screening system, and Rapiscan QXR1000 baggage and parcel screening system.

Summary

The ECP Pilot Program is underway, and completion of the ECP is expected in spring 2008. Combining the strategic design concepts presented herein with

GATEKEEPER

Gatekeeper: Under Vehicle Inspection System

The Gatekeeper is an under-vehicle inspection system with automatic alarming on anomalous objects. The undercarriage scanning system captures a high-resolution composite image of the entire undercarriage for comparison with previous scans. The software then highlights on the operator's screen any areas where differences have been found.

> http://www.gatekeepersecurity.com/about_us/overview.php/

System automatically places a red ring around foreign objects

RAPISCAN SECURE 1000

Rapiscan QXR1000

The Rapiscan Secure 1000 provides an effective personnel screening solution that produces high-resolution images that enable the operator to easily identify concealed threat and contraband items. It is ideal for high-security environments because it detects organic materials, such as explosives, and inorganic materials, such as metals.

Remote screening technology will be incorporated into the system for use at the ECP, enabling security forces to safely operate the screener from a distance.

> http://www.rapiscansystems.com/rapiscan_qxr1000_intro.html/

Rapiscan Secure 1000

relevant technologies provides a comprehensive capability set for US forces operating ECPs in theater.

For more information on the concepts and technologies used in the ECP Pilot Program, please contact the TSWG Physical Security Subgroup at pssubgroup@tswg.gov or via its web site (http://www.tswg.gov/tswg/ps/ps_ma.htm).

---

1 US Department of Defense. *Joint Forward Operations Base (JFOB) Force Protection Handbook*. Washington: Government Printing Office, 2005.

Editor's note: This article describes several available force protection material solutions and is not intended as an advertisement for these products.

Defense Critical Infrastructure Program (DCIP)

By LTC Pat Briley, DCIP lead in the Antiterrorism Branch, J-34 DDAT/HD on the Joint Staff at the Pentagon

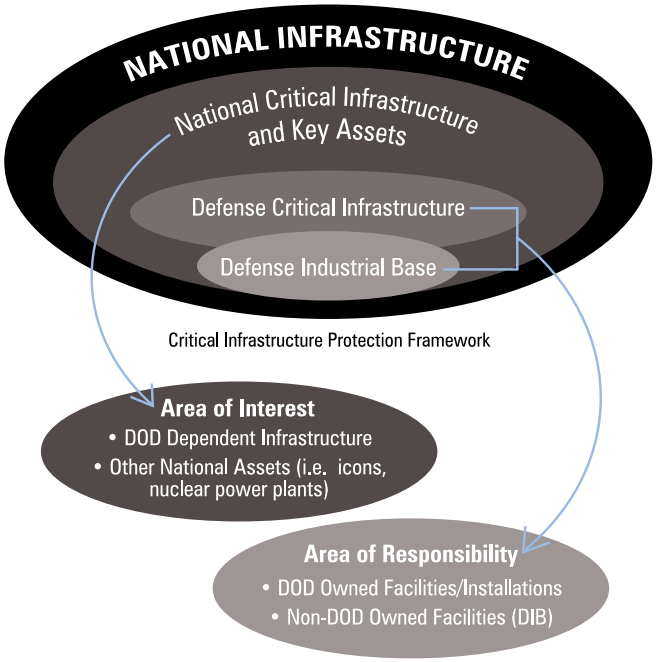
What is the Defense Critical Infrastructure Program (DCIP)? Ask 10 different people at the Department of Defense (DOD), the Joint Staff (JS), or a combatant command level, and they might just give 10 different answers—but not because they don't know. DCIP is one of DOD's newer programs, and it seems to be changing with every published policy document.

Infrastructure has always been associated with engineering, but DOD and the Joint Staff have taken infrastructure identification, prioritization, and protection to a whole new level. This article will attempt to show what the DCIP is, how it can serve other commands, and the way ahead for DCIP. Its focus is on DCIP from the military perspective (Defense Critical Infrastructure [DCI]) and will only touch on the wider spectrum that includes the Defense Industrial Base (DIB), Defense Sectors, and the Department of Homeland Security (DHS).

DCIP is a DOD risk management program that seeks to ensure the availability of networked assets critical to DOD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy (Department of Defense Directive [DODD] 3020.40, 19 August 2005). In essence, the DCIP is basically just a risk management program, but one that deals with the infrastructure and assets that are critical to DOD missions.

The Commander evaluates risk associated with his or her critical infrastructure and assets. Assets, as defined in the DCIP arena, are people, physical entities, or information owned or operated by domestic, foreign, public, or even private-sector organizations. Infrastructure is essentially the framework of networked assets that enable a continued flow of goods, information, and services.

What DCIP Is Compared To All National Infrastructure

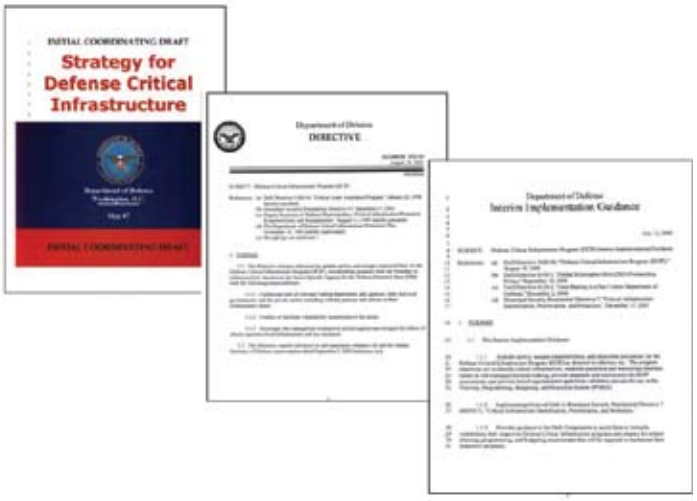


Policy

With the introduction of DODD 3020.40 in August 2005, the DOD established DCIP. Prior to that policy document, the DOD relied upon three documents: DODD 5160.54, Critical Asset Assurance Program, dated January 1998; Deputy Secretary of Defense Memorandum, Critical Infrastructure Protection Responsibilities and Realignments, dated August 1999; and the Department of Defense Critical Infrastructure Protection Plan, dated November 1998.

Homeland Security Presidential Directive (HSPD) #7, dated December 2003, established a national policy for federal departments and agencies to identify, prioritize, and protect critical infrastructure. HSPD #7 recognized that each infrastructure sector possessed its own unique characteristics and operating models and designated Sector-Specific Agencies (SSA). This document directed that DOD be the SSA for the Defense Industrial Base (DIB), which led to the writing of DODD 3020.40, and thus the cancellation of the previous DOD documents.

Critical Infrastructure Protection (CIP) and DCIP are commonly used interchangeably, but there is indeed a difference. For the CIP professional, whether government, civilian contractor, or military, the difference is apparent: CIP is a part of the overarching DCIP risk management program. For the majority of the public and corporate America, however, the difference between the two terms is minimal and, many times, irrelevant.



The Joint Staff, combatant commands, and the Services are currently working with the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs; ASD [HD&ASA]) to draft a Department of Defense Instruction (DODI) for DCIP. A placeholder DODI currently exists in the field, called the Interim Implementation Guidance (IIG), and that is set to expire in conjunction with the final approval and distribution of the new DCIP DODI 3020.40.

Many DOD documents in the field now help organizations, including DOD, Joint Staff, combatant commands, Services, Sectors, and component commands, understand the finer details of implementing a DCIP. The DOD, along with the Joint Staff and the Mission Assurance Division (MAD) in Dahlgren, Virginia, are authoring additional documents, many of which will be released in CY 2007. The Services are evolving their programs to match new DOD policy and guidance and, in most cases, assisting DOD in developing new policy and doctrine.

Establishment and Identification of Criticality

Early in the evolution of the DCIP, several methods were used to determine criticality. In the absence of a DOD policy or instruction on criticality establishment, the Services and the combatant commands developed their own methods. The CIP community used creativity and initiative to solve the initial problem but created another. DOD found itself trying to establish a DOD-wide criticality process and, at the same time, using methodology that was already established within the Services and combatant commands.

The level of criticality of a particular asset or infrastructure depends on the level of command in which it is found and how it is to be used. At the strategic DOD level, a true critical asset is called a Defense Critical Asset (DCA) and is defined as "an asset of such extraordinary importance to DOD operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of DOD to fulfill its mission" (DCIP Criticality Process Guidance Document [CPGD], December 2006).

The Joint Staff, with the help of the five geographic combatant commands and four functional combatant commands, has compiled a list of the combatant commands' Task Critical Assets (TCA). A TCA is simply a DCA at the combatant command level and is further defined as "a task asset that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability to execute the task it supports [combatant command level]" (DCIP CPGD, December 2006).

Within the list of TCAs are also those submissions from the Services that ensure that the Services' Title X functions of organize, maintain, equip, train, recruit, and so forth, are covered. Not all of the Services had submitted their lists as of this writing, but the lists are anticipated by late summer 2007.

Prioritization

The lists of TCAs will greatly assist senior civilian and military leadership make informed decisions and provide situational awareness in the event of a natural disaster or attack. The Joint Staff is in the process of analyzing the combatant commands' TCA submissions. After receiving the Service TCAs, it will nominate a portion of the TCAs to the ASD (HD&ASA) to become DCAs. This list of DCAs, along with supporting data, will determine the scheduling of DCIP assessments for CY 2009 and beyond and will routinely receive visibility at the highest levels of government due to its strategic value.

The current list of just over a thousand TCAs will not be prioritized numerically. Instead, it will be split into three categories (or tiers) based on association with supported Joint Mission Essential Tasks (JMETs) and Operational Plans (OPLANs) from the respective combatant commands. The current list of TCAs was submitted from each of the combatant commands at the request of the Joint Staff. In the future, all DCIP offices will use service-oriented architecture (SOA) or web services to pull pertinent combatant command, Service, and Sector data at a moment's notice, thereby getting the most current information. All TCAs are now available on the web for all authorized users to see and use as applicable and as appropriate.

With the approval and publishing of the new DCIP Security Classification Guide, the DCAs, once approved by the ASD (HD&ASA), will be available only on the Joint Worldwide Intelligence Communications System (JWICS) for select personnel due to their classification. All of the TCAs, however, are on a SIPRNET-based platform, yet to be named, but closely related to the US Strategic Command's (STRATCOM) Strategic Mission Assurance Data System (SMADS).

The Joint Staff is currently researching whether to put more of the data on JWICS as well as additional DCAs, including limited DOD Continuity of Operations (COOP) data. In order for the data to be worthwhile, it must be accessible and easy for all customers to use, but security precautions as per the new classification guide must be followed to the fullest extent.

Vulnerability Assessments

The Joint Staff began conducting Joint Staff Integrated Vulnerability Assessments (JSIVAs) as a result of the Khobar Towers terrorist attack on 25 June 1996. The main objective of the assessments is antiterrorism and force protection; however, it was discovered early on that the assessments did not adequately cover critical infrastructure.

DOD recognized the gap in coverage and created a pilot program for DCIP assessments. A team of four CIP professionals was attached to a JSIVA team to look solely at DCI from a mission assurance perspective. This team looked at all hazards, including not only terrorist attacks but insider attacks, natural disasters, utility malfunctions, and any other event that would degrade or cause mission failure. The DCIP module is not to be confused with the Balanced Survivability Assessment (BSA) which is an in-depth look at a mission and usually is conducted over the span of two to three weeks.

DCIP is a DOD risk management program that seeks to ensure the availability of networked assets critical to DOD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy.

The DCIP pilot assessments began in 2005 at Fort Bragg, North Carolina, and subsequent assessments were conducted at Bangor International Airport, Maine; Fort Detrick, Maryland; Land Naval Support Activity, Pennsylvania; Camp As Saleyiah, Qatar; and Camp Pendleton, California. Each Service was the subject of at least one DCIP assessment. The sites were selected based on the 2005 JSIVA schedule and included various types of missions, including force projection, logistics, and information operations.

The successful pilot assessments led the Defense Threat Reduction Agency (DTRA) to use contractors attached to two of the six JSIVA teams. The teams conducted 20 assessments in 2006 and are conducting 20 in 2007. The results of the DCIP assessments are almost always classified SECRET and could identify vulnerabilities that could prevent a combatant command from fulfilling a critical function or capability.

The standards and benchmarks for the DCIP assessments were written before the pilot assessments and have changed substantially since their initial release. The current list of standards and benchmarks, updated in May 2007, can be found in the new DCIP DODI and can be downloaded from the Antiterrorism Enterprise Portal (ATEP).

2007 Assessment Schedule	
Vandenberg AFB, California	February/March
Port of Jacksonville, Florida	March
Soto Cano Air Base, Honduras	April
Fort Richardson, Alaska	April
Naval Air Station, Key West, Florida	April
Port of Beaumont, Texas	May
Port of Charleston, South Carolina	May
Port of Norfolk, Virginia	May
Kunsan Air Base, Republic of Korea	June
Fort Campbell, Kentucky	June
MCAS Cherry Point, North Carolina	June
Vilseck-Grafenwoehr, Germany	August
Fort Bliss, Texas	August
Naval Station, Rota, Spain	August
COMNAVMARIANAS, Guam	September
Shariki, Japan	September
Fort Greely, Alaska	September

2008 Assessment Schedule

Adak, Alaska
Andersen AFB, Guam
Fort Bragg, North Carolina
Offutt AFB, Nebraska
Port of Tacoma, Washington
Port of Wilmington, North Carolina
Robins AFB, Georgia
Daegu Base Cluster, Korea
Tyndall AFB, Florida
Tinker AFB, Oklahoma
Fort Detrick, Maryland
Marine Corps Logistics Base, California
Naval Air Station, Atsugi, Japan
Fort Buckner, Okinawa Japan
Elmendorf AFB, Alaska
Eareckson Air Station, Alaska
Camp Lejeune, North Carolina
Raven Rock Complex, Pennsylvania and Maryland
Camp Pendleton, California
Andrews Air Force Base, Maryland

DCIP Technologies

ATEP

ATEP is the "one-stop shopping" portal for the entire Antiterrorism/Force Protection and DCIP community. ATEP (both NIPRNET and SIPRNET) has a section under "Communities," called "CIP," where the Joint Staff routinely places policy documents (draft and approved), working group documents, JSIVA and DCIP assessment schedules, and many different types of DCIP information.

The CIP section of ATEP is the key place for all DCIP information from the combatant command level to the unit level. It is updated on a weekly basis and membership must be requested. The J-34 AT Branch CIP professionals are responsible for this area within ATEP. Additionally, many of the combatant commands and Services have their own DCIP communities where their policies and instructions are stored, as well as information about conferences, working groups, and assessments. The ASD (HD&ASA), the DOD proponent for CIP, also has a web page on the NIPRNET with CIP information and links to other CIP sites.

The Core Vulnerability Assessment Management Program (CVAMP) is a database accessible through the ATEP SIPRNET portal and contains all of the JSIVA and DCIP assessment reports. The DODI 2000.16 directs that the heads of DOD components use CVAMP, and it is the only database that has complete histories of vulnerability assessments; it also has combatant command and Service command integrated vulnerability assessment data. Membership is required to access the data. The main purpose of CVAMP is to track resources against identified vulnerabilities using Combating Terrorism Readiness Initiatives Funds (CbT-RIF) and unfunded requirements (UFR). The DCIP assessments were added in 2006 and are currently read-only.

Asset Characterization Tools

Many asset characterization tools are available. One of the most popular seems to be the Critical Asset Management (CAMs) platform, created by Booz Allen Hamilton through research and development with the US Marine Corps (USMC). The US Air Force (USAF) and the US Army have adopted CAMs, and the US Navy (USN) is seriously considering using it.

Each military base, installation, post, and so forth has its own asset characterization tool to track force protection and other areas. The USAF uses GeoBase, the USMC uses GeoFidelis, the USN uses GeoReadiness, and the USA uses Installation Geographic Information and Services (IGI&S). Those geospatial systems are used primarily "within the wire" of a military compound, unlike the CAMs system, which goes beyond the installation perimeter. All of the systems can be accessed online from the Defense Installation Spatial Data Infrastructure (DISDI) portal (http://www.acq.osd.mil/ie/bei/disdi.htm).

STRATCOM created its own, unique system, called the Strategic Mission Assurance Data System (SMADS). The USMC and STRATCOM have led the combatant command and Service efforts in asset characterization. Both CAMs and SMADS are promising systems as long as the Defense Readiness Reporting System (DRRS) can access the data through net-centric operations that push the DCIP data to report on level of readiness. DRRS is in the future for DCIP, and it will be totally integrated. All of the systems developed today must be designed with DRRS in mind.

Assessor Tools

An abundance of technological tools exist for the CIP professional and assessor to use in his or her daily duties. Science Applications International Corporation (SAIC) has created the Mission Assurance Toolkit (MAT). MAT is primarily used on DCIP assessments to collect very specific data, including latitudes and longitudes and photos of TCAs and other critical infrastructure. It also does limited analysis and geospatial viewing on a hand-held device. Nearly all of the data collected will go into a central repository at the MAT in Dahlgren, Virginia, for further analysis.

Several financial institutions on Wall Street, major commercial power-generating plants, and key bridges and canals are but a few examples that would be considered critical infrastructure.

Homeland Infrastructure Foundation-level Database

The Homeland Infrastructure Foundation-level Database (HIFLD) was created several years ago in a nascent CIP community. It brings DOD and non-DOD organizations together with a goal of consolidating common data elements regarding infrastructure. It also serves as a working group in which entities can share their ideas on infrastructure tracking, geospatial visualization, and readiness. Since its creation, the CIP community has discovered much duplication of effort and is using HIFLD to collaborate with colleagues from labs and government agencies, both DOD and non-DOD.

Other Technologies and Platforms Around the CIP Community

Other systems and tools are also available for use by combatant commands, Services, and defense agencies. The Pacific Command (PACOM) DCIP office is currently using a remote data collection capability to record asset locations and answers to questions related to respective benchmarks for DCIP assessment of assets. Data is collected using a hand-held device that doubles as a GPS receiver and is compatible with ESRI mapping suites.

The Homeland Data Sharing Program (HDSP) was developed as a result of Hurricane Katrina and is the sharing portal for non-DOD entities. It allows them to share not only critical infrastructure information, but also data on disease outbreaks, natural disasters, and other events. HDSP is currently a directory on the Homeland Security Information Network (HSIN) and requires registration for membership.

The Homeland Defense Operational Planning System (HOPS) is a web-accessible system that provides situational awareness for risk management and tools for critical infrastructure that may be affected by deliberate attack or natural disaster.

For geospatial visualization of CIP data, SMADS currently has all of the TCAs available for authorized users. Palanterra and HD-Map, both on the SIPRNET, also have limited TCA data available for those who can access the systems.

CIP Training

Many colleges and universities now teach courses on CIP. The US Joint Forces Command (JFCOM) is currently working on CIP training within the DOD community, and the West Virginia Army National Guard is currently teaching DCIP assessor classes at Camp Dawson. The Navy Post Graduate School currently has an excellent online CIP training course, which could prove very beneficial to the newcomer in the CIP community.

Non-DOD CIP Information

DOD does not have the market cornered on critical infrastructure. Several financial institutions, major commercial power-generating plants, and key bridges and canals are but a few examples that would be considered critical infrastructure. The DOD partners with the DHS in the monitoring of critical infrastructure. The National Infrastructure Coordinating Center (NICC), located in Herndon, Virginia, maintains operational awareness of the nation's critical infrastructure and key resources and provides a mechanism and process for coordination between government and industry. The Homeland Security Operations Center (HSOC) is a watch center, similar to the many that DOD operates; it communicates daily with the 10 sectors and, most importantly, the US Northern Command (USNORTHCOM).

Much like the Joint Staff's TCA database, DHS has its National Asset Database (NADB). NADB is a repository and inventory for nonmilitary national

infrastructure and resources and is housed at Oak Ridge National Laboratory; a classified version of this database is available on the SIPRNET. DHS's database system will more than likely be linked to DOD's system of choice in the near future to ensure that senior decision makers, both military and civilian, can make informed decisions on risk management and consequence management.

Summary

This article is not meant to be an all-inclusive profile of CIP but more a "slice-in-time" look. In a year from this writing, the community will have evolved and will look quite a bit different. With technology changing at a rapid pace, the CIP community must also change to keep up with technology and, more importantly, with the many threats to our very existence.

Identifying and Defeating Infiltration Threats to the Homeland

By Lt Col Michael T. Imbus, Air Force Office of Special Investigations (AFOSI) Special Agent, and former Counterintelligence Staff Officer (CISO) at the United States Transportation Command (USTRANSCOM) and senior counterintelligence advisor to the USTRANSCOM Commander

Although the United States has dedicated considerable effort to countering terrorist threats to the homeland, these measures have not addressed the full range of infiltration threats faced by the nation. This paper proposes an analytical framework for examining the full range of infiltration threats posed by both state and nonstate actors.

This framework can be used to assess an adversary's presence in the United States and the ease with which their nationals can access US society; their ability and intent to conduct aggressive intelligence operations within the United States; the collection priorities of their espionage operations; their military special operations capabilities; and the nature of their military doctrine and focus on asymmetric operations. The applicability of this analytical framework is demonstrated via an examination of Chinese infiltration capabilities. This examination explores the likelihood that China would have the ability and intent to conduct terrorism, assassinations, sabotage attacks, and espionage operations within the United States in the event of military conflict.

Counterintelligence (CI) is one of the primary tools that can counter infiltration threats, but unfortunately the US Intelligence Community has generally treated CI as an adjunct requirement and failed to develop adequate attention and resources for this essential discipline.[1] Despite the changes in the threat environment in the post–Cold War and 9/11 era, the Department of Defense (DOD) continues to focus the bulk of its intelligence effort on foreign intelligence activities and devotes minimal resources to CI activities.[2] This paper calls for a reevaluation of the balance between US government foreign intelligence and CI resources, and continued enhancement of the links between counterterrorism and CI efforts.

A Framework for Analyzing Foreign Infiltration Threats

DOD has long had a framework for analyzing terrorist threat levels in foreign countries that host US forces or serve as transit points. This framework quantifies the terrorist threat in a given country as Negligible, Low, Medium, High, or Critical. To determine the terrorist threat level in a given country, a minimum of five factors are considered: terrorist-group existence, capability, history, trends, and targeting.[3]

In the post–9/11 environment, Americans have become familiar with the color-coded Homeland Security Advisory System instituted by Homeland Security Presidential Directive-3 in March 2002.[4]

Although both of these frameworks provide useful information, they focus exclusively on terrorism conducted by nonstate actors and thus ignore the threat posed by espionage, sabotage, or assassination operations conducted by foreign nations. This paper seeks to augment the existing DOD and Department of Homeland Security (DHS) terrorist assessment tools by introducing an analytical framework for examining the full range of foreign infiltration threats.

Determining the full-spectrum infiltration threat to the United States posed by potential adversaries

requires the examination of several factors. First, the adversary's current official and unofficial presence in the country and their ease of access to the US homeland must be determined. Do they maintain diplomatic facilities, such as an embassy, consulates, or trade offices, in the United States? Do they send large numbers of students to study at US universities or colleges? Do they have a robust merchant marine or national airline that allows their nationals to routinely operate at important US airports and seaports? Do they send business, trade, or scientific delegations to the United States?

Next, the intelligence capabilities of the potential adversary must be studied. Have they demonstrated the ability to conduct sophisticated espionage operations against the United States? Do their external intelligence services maintain a paramilitary capability? What is the relationship between the intelligence service and military special operations forces? Do they work together to conduct reconnaissance, gather intelligence, and covertly infiltrate operatives into targeted areas, or are they stifled by rivalry and distrust?

Unfortunately, determining foreign intelligence collection priorities is complicated because the United States can never hold perfect knowledge of an adversary's intelligence activity. Intelligence collection is a clandestine activity, and intelligence operatives go to great lengths to mask their endeavors. CI professionals operate in an ambiguous world where things are not always what they appear. For this reason, US CI agencies must constantly ask themselves a fundamental question: Is country X's apparent lack of interest in a particular category of collection targets a reflection of reality, or is it merely a result of the US CI Community's inability to penetrate the foreign service and ascertain their true intentions?

Finally, the potential adversary's military doctrine and the capabilities of their special operations forces (SOF) should be examined. Does the country's military doctrine stress asymmetrical attacks against strategic targets in the enemy's rear area? Do they maintain SOF units capable of covertly infiltrating a target area and successfully striking key command and control facilities, transportation nodes used to deploy military forces, or essential military installations? Have they carried out successful sabotage operations in the past? Does the country maintain ongoing relationships with international terrorist organizations that could augment their SOF capabilities by acting as proxies to conduct attacks against the United States?

Counterintelligence (CI) is one of the primary tools that can counter infiltration threats, but unfortunately the US Intelligence Community has generally treated CI as an adjunct requirement and failed to develop adequate attention and resources for this essential discipline.

Third, studying a potential adversary's intelligence collection priorities can provide insight into their future plans. A country that devotes considerable effort to monitoring its own nationals or dissidents abroad reflects a focus on internal security and likely poses little direct espionage or sabotage threat to the United States. A country that focuses on collecting intelligence related to military capabilities, plans, and intentions is probably doing so for conventional military and defense purposes. Collecting data on advanced science and technology programs allows a country to build its own capabilities without paying high research and development costs, and gathering data on advanced weapons systems can enable an adversary to develop tactics, techniques, and procedures to defeat these weapons. Collecting political intelligence can improve a country's ability to meet its goals and objectives during international negotiations. On the other hand, a potential adversary that devotes a significant percentage of its intelligence collection efforts to gathering data on vital defense installations, critical transportation infrastructure, and large population centers may be collecting targeting data. Because few countries possess the capability to strike at the US homeland with conventional military forces, this intelligence could be used to support contingency planning for sabotage, assassination, or terrorist attacks.

The analytical framework presented in this paper offers a tool for examining the full range of infiltration threats to the homeland. It is applicable to any state actor and, with slight modification, can be used to evaluate the infiltration threat posed by a nonstate entity such as a transnational terrorist organization.

Analyzing the Infiltration and Sabotage Threats Posed by the People's Republic of China

To demonstrate the utility of the analytical framework presented in this paper, it is helpful to apply it to a potential adversary. The People's Republic of China (PRC) is used for illustrative purposes based on a number of factors. First, as recognized by the February 2006 *Quadrennial Defense Review Report,* China is the most likely member of the international community to emerge as the next peer or near-peer competitor of the United States.[5] Second, China maintains a robust diplomatic presence in the United States, and the increasing economic ties between the two countries provide Chinese businessmen, merchant mariners, and students regular and routine access to the US homeland. Third, China

continues to conduct aggressive intelligence collection operations against the United States and enhance the capability of its military special operations forces.[6] Finally, recent Chinese military doctrine and thought has stressed the concept of using asymmetric attacks to defeat a stronger enemy and raised the idea of unrestricted warfare, which does not differentiate between military and nonmilitary targets.[7]

China's Presence in the United States

The first step in evaluating the infiltration threat posed by a particular nation state is to examine that country's presence in the United States. China maintains an embassy in Washington, DC, and consulates in San Francisco, Los Angeles, New York, Houston, and Chicago.[8] In addition to these establishments, the PRC maintains a Permanent Mission to the United Nations in New York.[9] This robust official presence provides the PRC with ample opportunity to infiltrate intelligence personnel into the United States.[10] As of 1994, approximately 1,500 PRC diplomats and official commercial representatives were living and working in the United States. Stanislav Lunev, a former Soviet intelligence officer who was previously assigned to Beijing and who defected to the United States in 1992, estimates that two-thirds of all permanent Chinese diplomatic positions in foreign countries are filled by intelligence personnel.[11] If these figures are accurate, at any given time the PRC has 1,000 trained, professional intelligence personnel operating in the United States under official cover.

In addition to the personnel who staff PRC embassies, consulates, and other official establishments, China can potentially capitalize on the large number of Chinese students who attend US universities and colleges. The Institute of International Education reported that there were 62,523 Chinese students studying in the United States during the 2004–2005 academic year.[12] Although it is unrealistic to expect that all or even a majority of these students are actually professional intelligence agents or sabotage operatives, this large pool of potential recruits provides China with an incredibly valuable tool for gathering basic intelligence within the United States. The existing presence of large numbers of Chinese students could also allow China to infiltrate large numbers of operatives into the United States without drawing undue attention from US CI and security agencies.

Growing trade between China and the United States has resulted in numerous Chinese companies operating in the United States. Based on the nature of the Chinese political and economic system, it is difficult to separate these companies from the Chinese government. The China Ocean Shipping Company (COSCO), one of the world's largest maritime shipping businesses, provides an example of Chinese state-owned commercial activity in the United States. COSCO vessels make routine visits to US seaports, including some of the strategic locations used to deploy US military forces in times of crisis. According to the Federal Maritime Commission, COSCO maintains a fleet of more than 600 ships that call at 1,100 ports in 150 countries. COSCO uses 59 transportation hubs in North America and makes weekly calls at the ports of Baltimore, New York, Charleston, Houston, Long Beach, Seattle, Oakland, and Norfolk.[13] According to Senator James Inhofe (R-Oklahoma), COSCO is owned by the Chinese People's Liberation Army and functions as the merchant marine of the Chinese military.[14] Air China, the flag airline of the PRC, provides passenger and cargo service between China and several US cities. Air China passenger and cargo flights routinely travel to Los Angeles, San Francisco, and New York. In addition to these locations, Air China offers cargo service to Chicago and Portland, Oregon.[15] These facts clearly demonstrate China has multiple channels for easy access to the United States.

A potential adversary that devotes a significant percentage of its intelligence collection efforts to gathering data on vital defense installations, critical transportation infrastructure, and large population centers may be collecting targeting data ... this intelligence could be used to support contingency planning for sabotage, assassination, or terrorist attacks.

PRC Intelligence Operations

According to the Federal Bureau of Investigation (FBI), China currently poses a more significant intelligence collection threat to the United States than any other country.[16] China's primary civilian intelligence agency is the Ministry of State Security (MSS). The MSS was established in 1983 and is responsible for collecting intelligence within foreign countries and conducting CI activities in China and abroad.[17] In addition to the MSS, China maintains a military intelligence collection capability. The Military Intelligence Department of the People's Liberation Army General Staff is responsible for collecting foreign intelligence and military and technological information.[18]

Chinese intelligence agencies have demonstrated the ability to use both official and nonofficial cover positions to allow their case officers to operate outside China's borders.[19] This ability allows them to capitalize not only on the Chinese diplomats and military attachés working in the United States and official delegations visiting the country, but also

to exploit the Chinese students, businessmen, journalists, merchant seaman, and scientists who visit the United States. In a joint FBI and Central Intelligence Agency (CIA) report to Congress, US CI officials highlighted China's history of using Chinese students to gather intelligence information and pointed out China's use of its growing commercial presence in the United States to enhance its intelligence collection capabilities.[20] It is estimated that over 3,000 Chinese front companies conduct espionage activities in the United States.[21]

Although capable of mounting sophisticated, clandestine collection operations against the United States, Chinese agents frequently exploit information legally available from Western publications, US university libraries, unclassified databases, US research institutions, and the internet.[22] In addition to traditional human intelligence collection operations, China is suspected of conducting aggressive computer network operations in an effort to obtain sensitive information. Chinese hackers have reportedly penetrated sensitive DOD and other US government information systems, as well as US government contractor systems. In addition to allowing China to obtain large amounts of sensitive data, this effort could provide Chinese information warfare specialists with background information that would allow them to degrade, shut down, or exploit US computer systems during a crisis.[23]

Chinese Intelligence Collection Priorities

China devotes significant effort to gathering a broad spectrum of intelligence information from the United States. China is keenly interested in gathering science and technology information to advance its growing economy and seeks political intelligence on US foreign policy developments and intentions.[24] In addition, Chinese leaders recognize US military superiority and seek to obtain US military and military-related technology. Chinese intelligence operations have successfully obtained information on advanced US thermonuclear warheads and space and missile technology, including advanced guidance systems, high-powered computers, advanced machine tools, and jet engines.[25]

There is no publicly available information that indicates Chinese agents have been detected gathering information on the physical attributes and security of US military and other government facilities, population centers, communication nodes, transportation infrastructure, and other likely sabotage targets. Instead of indicating a lack of Chinese interest in these types of targets, this void could simply mean that China is using less risky, legal methods to gather this type of data. As an open society, a great deal of information on US installations, transportation facilities, and key landmarks is publicly available. China has no need to send trained intelligence professionals to gather this type of data when it can be easily obtained by an open-source intelligence specialist via an internet connection in Shanghai or collected by a merchant seaman or commercial airline pilot who visits these facilities in the course of his normal duties. The sheer number of Chinese diplomatic personnel, students, and business officials living in and visiting the United States makes it impossible for US CI agencies to monitor their activities. Reviewing other nations' foreign collection efforts illustrates the importance of monitoring Chinese and other foreign nationals residing in the United States.

During the late 1990s and early 2000s, US CI professionals caught personnel assigned to the Iranian Mission to the United Nations conducting apparent photographic and video surveillance of key landmarks and transportation infrastructure in New York, including the Statue of Liberty, Rockefeller Center, the Brooklyn Bridge, the Queens–Midtown Tunnel, a subway station, the Staten Island Ferry Terminal, and Metropolitan Transit Authority buses.[26] Other than the UN Mission, the only Iranian diplomatic facility in the United States is a small Iranian Interest Section located in the Pakistani Embassy.[27] The small number of Iranian diplomats in the United States makes it relatively easy for US CI to track and monitor them. Iran's identification as a member of the "Axis of Evil" and the country's history of sponsoring terrorist attacks against US interests likely makes Iranian diplomats a primary focus of the FBI and other US CI agencies. Unlike their Iranian counterparts, Chinese intelligence officers and agents operating in the United States do not face this same level of scrutiny; they could theoretically collect data on potential sabotage targets while avoiding detection.

PRC Special Operations Capabilities

The Chinese military has a limited history of maintaining dedicated SOF units and has no recent history of conducting complex sabotage and assassination operations outside China's borders. Additionally, China is not considered a state sponsor of terrorism, and there is no information to indicate Chinese intelligence or SOF personnel maintain ongoing relationships with terrorist organizations.[28] The People's Liberation Army (PLA) fielded its first dedicated SOF unit in 1988.[29] As of 2005, each of the seven PLA military regions possessed regiment-sized SOF units.[30] In his book, *Interpreting China's Military Power,* Ko Po Ng states that Chinese SOF "are mainly trained in special reconnaissance, sabotage assaults, infiltration, guerrilla warfare, psychological operations and information operations." Ng goes on to state that those forces could be used to "attack enemy C4ISR centers and seize key air- and seaports."[31]

Other authors have stressed that PLA SOF focus on conducting direct action and special reconnaissance missions.[32] As of 2005, 25,000 SOF operators were in the Chinese Army and another 1,500 were in the PLA Marine Corps; in addition, the PLA Air Force Airborne Corps maintained an unknown number of SOF battalions comprised of 400 to 500 operators.[33]

As a comparison, in 2004 the US military had approximately 34,000 active-duty SOF operators with an additional 15,000 assigned to the reserve components; the CIA also reportedly maintained a force of 150 SOF operators in its Special Activities Division.[34] North Korea maintains what arguably constitutes the largest Special Forces contingent in the world: experts estimate that in 1998 the North Korean People's Army had over 100,000 SOF operators, augmented by large numbers of special operations–trained personnel assigned to North Korean intelligence agencies.[35] Iran has taken a different approach in its efforts to develop asymmetric capabilities. Although Iran maintains relatively small numbers of dedicated SOF, Iran's active support of and relationships with key terrorist organizations provide the country with an impressive asymmetric capability. The United States Government in 2005 identified Iran as the international community's most active state sponsor of terrorism.[36] At that time, the Iranian army had one SOF division of approximately 5,000 men, and the Iranian Revolutionary Guards Corps (IRGC), or Pasdaran, also maintained a 5,000-man SOF division. The IRGC Quds Force augments these forces. Although the size and budget of the IRGC Quds Force is unknown, they are known to operate from Iranian diplomatic facilities located in foreign countries.[37] The IRGC serves as the primary Iranian Government interface with terrorist organizations such as Hezbollah and Hamas, and Iran relies on these organizations to conduct sabotage and terrorist actions on behalf of the regime.[38]

Chinese SOF lack the long history and full capabilities of their American counterparts, the numbers of SOF operators fielded by the North Korean People's Army, and the long-term connection with terrorist proxies enjoyed by the Iranian IRGC. Despite these facts, China has taken steps to enhance the SOF competencies of its military forces and invested some of its best people and most advanced equipment to develop and field SOF capabilities.[39] For these reasons, it would be a mistake for US defense officials to ignore Chinese SOF threats. China's growing SOF capabilities, coupled with its existing intelligence capabilities and robust presence in the United States, provides it with the basic capabilities needed to conduct sabotage strikes or assassination operations within the US homeland. To determine the likelihood of China using those capabilities in a conflict with the United States, Chinese military doctrine must be examined.

As China has increased the of its national interests, reexamine its security

PRC Military Doctrine

In addition to developing enhanced SOF capabilities, Chinese military professionals have developed doctrine that highlights traditional SOF missions and strengths. As China's economic strength and role in the international community has grown, its military leaders have sought to develop and adopt a military doctrine that reflects the country's status in the current international security order. Early Chinese Communist military doctrine stressed the strengths provided by China's territorial size and large population. The "People's War" concept of Maoist China emphasized "mass and defense in depth" while sacrificing "operational readiness for structural readiness."[40] Chinese defense leaders have steadily moved away from this defensive doctrine. Early Chinese defense policies and military doctrine focused exclusively on ensuring the survival of the PRC and maintaining its territorial integrity. Chinese national interests have grown to include not only the preservation of Chinese sovereignty and territorial integrity, but also ensuring the stability of the international order, maintaining and strengthening China's role in foreign affairs, safeguarding economic interests, expanding export markets, and maintaining access to overseas resources. As China has increased the external dimensions of its national interests, it has been forced to reexamine its security posture.[41]

external dimensions it has been forced to posture.

Three constants have survived the refinement of Chinese military doctrine from 1949 to present. The first constant is the preeminent position of PLA land forces in the Chinese military. Even today, the PLA Naval and Air Forces play a supporting role to their counterparts in the PLA land forces and serve as their "junior partners."[42] The second is the long-term Chinese attraction to using asymmetric capabilities to target enemy weaknesses or to turn an enemy's strength against itself.[43] Finally, Chinese leaders have consistently viewed the United States as a potential threat. In an article entitled, "The PLA in a Changing China: An Overview," Stephen J. Flanagan and Michael E. Marti state: "The PLA military strategy sees the United States as its principal adversary. As a result, the PLA increasingly emphasizes preemptive, asymmetric strikes against critical American military targets, as well as active and passive defenses against US long-range precision strike systems."[44]

Chinese military officers have produced books and articles expounding on the use of preemptive and asymmetric attacks to defeat stronger adversaries. Although those works may not reflect official Chinese military doctrine, their publication under the auspices of the PLA reflects the belief of Chinese military officials that the works hold at least some degree of merit. In February 1996, Lu Linzhi published an article in the Liberation Army Daily calling on Chinese military leaders to launch preemptive strikes in the event that war with a stronger power becomes inevitable. Although Lu does not specifically identify the United States as the focus of his article, it is easy to conclude from the context of the article that the United States is the potential enemy referenced in his work. Lu praises the success of the Israeli forces in the 1967 Six-Day War and faults Saddam Hussein for failing to seize the initiative in the first Gulf War by not conducting a preemptive strike against US forces. Lu recognizes that the United States "is most vulnerable during the early phase of the war when it is still deploying troops and making operational preparations." Lu states this is the point China should launch an overwhelming strike using "fire assaults, special operations, and sabotage operations." Lu writes that in determining the targets for these strikes, Chinese forces "should zero in on the hubs and other crucial links in the system that moves enemy troops as well as the war making machine, such as harbors, airports, means of transportation, battlefield installations, and the communications, command and control, and information systems."[45]

Colonels Qiao Liang and Wang Xiangsui created a stir with the 1999 publication of their book *Unrestricted Warfare*. When interviewed by a reporter from the Chinese Communist Party Youth League, Colonel Qiao stated, "The first rule of unrestricted warfare is that there are no rules, with nothing forbidden."[46] Unrestricted warfare transcends the boundaries between the worlds of war and nonwar and does not differentiate between military and nonmilitary targets. The concept of unrestricted warfare stresses the use of asymmetric methods to "find and exploit an enemy's soft spots." The proponent of unrestricted warfare should strike where his "adversary does not expect to be hit" and should focus attacks on locations that "will result in a huge psychological shock to the adversary." Qiao and Wang state that the US military is ill-prepared to confront an enemy who engages in unrestricted warfare because US defense officials "have never taken into consideration and have even refused to consider means that are contrary to tradition and to select measures of operation other than military means."[47]

Rating the Infiltration Threat Posed by China

Using the analytical framework presented in this paper and information available from open sources, it is possible to evaluate and rate the infiltration threat China could pose to the US homeland in the event of hostilities. For illustration purposes, the familiar five-tier scale of the current DOD terrorism matrix, which characterizes terrorist threats as Negligible, Low, Medium, High, or Critical, can be used to describe infiltration threats. The large number of Chinese citizens living, working, and studying in the United States would lead to a "High" rating in the Presence category. This rating reflects the reasonable assumption that clandestine Chinese intelligence agents and operatives are already present in the United States. China's demonstrated ability to conduct sophisticated clandestine intelligence operations and its current status as the single greatest espionage threat to the United States would result in a "Critical" rating in the area of Intelligence Operations. On the other hand, the observation that Chinese intelligence agencies do not currently focus their collection efforts on gaining information that would allow them to plan sabotage, assassination, or terrorism operations would result in a "Low" rating in the area of Intelligence Collection Priorities. China's growing

SOF capabilities provide a pool of highly trained operatives able to covertly operate within US borders to conduct sabotage and other direct-action missions. Despite this fact, China lacks a long-term history of conducting successful SOF strikes outside its borders and lacks access to terrorist proxies to augment its SOF capabilities. For this reason, the Chinese would receive a "Medium" rating in the SOF Capabilities category. Finally, China's emerging military paradigm stressing unrestricted warfare and the importance of conducting preemptive, asymmetrical strikes against a stronger enemy would lead to a "Critical" rating in the Military Doctrine category. Consolidating the ratings in the separate categories would result in an overall infiltration threat rating of "High."

Recommendations and Conclusions

The US government has devoted significant energy and financial resources to counter terrorism in the post–9/11 environment. Although these antiterrorism measures are a step in the right direction, the United States has not yet taken actions to address the full spectrum of infiltration threats to the homeland. To identify and understand the infiltration threat to the United States, the US intelligence and security communities must move beyond current analytical methodologies and threat advisory systems focused solely on terrorism. An analytical framework must be developed that examines the full spectrum of infiltration threats, including terrorism, sabotage, assassination, and espionage. Simply put, it is impossible to counter a threat one does not understand. The analytical framework presented in this paper provides a starting point for expanding US government analytical efforts from terrorism to all categories of infiltration threats.

CI is one of the primary tools that can counter infiltration threats, but unfortunately the US intelligence community and DOD have generally treated CI as an adjunct requirement and failed to devote adequate attention and resources to this essential discipline.[48] Although the threat environment has drastically changed over the past 20 years, the resource balance between foreign intelligence and CI activities across DOD remains essentially unchanged from the Cold War era. This balance needs to be reevaluated. In an era when terrorism and other asymmetric threats serve as the primary threat to the homeland, it no longer makes sense for DOD to devote the vast majority of its intelligence resources to foreign intelligence activities and only minimal resources to CI.

As the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction noted, "counterintelligence has generally lost stature since September 11, eclipsed by more immediate counterterrorism needs."[49] As the lead agency for both CI and counterterrorism efforts within the United States, the FBI should continue to play a major role in countering the full range of infiltration threats. The FBI has taken positive steps to enhance the interaction between FBI personnel conducting CI and counterterrorism investigations.[50] The FBI should continue this trend by expanding the charter of the current Joint Terrorism Task Forces (JTTFs) to include the traditional CI missions of countering foreign-directed espionage, sabotage, and assassination operations. These organizations should transition from JTTFs to Joint National Security Task Forces (JNSTFs) and hold primary responsibility for investigating the full spectrum of infiltration threats to the homeland, including transnational terrorism, international criminal activity, state-sponsored terrorism, sabotage operations, assassination, and espionage, and other foreign intelligence activities. The task forces would continue to be led by the FBI and include representatives from DHS; DOD; and other federal, state, and local law enforcement and security personnel. DOD CI agencies and the Defense Criminal Investigative Organizations should continue to maintain and expand their presence within the FBI-led task forces.

By better analyzing and understanding infiltration threats, expanding the CI resources devoted to countering those threats, and continuing to enhance the connection between CI and counterterrorism activities, the US government can improve its ability to counter the full range of infiltration threats and more effectively protect the homeland.

---

1. Commission on the Intelligence Capabilities of the US Regarding Weapons of Mass Destruction, *Report to the President of the US* (Washington DC: Commission on the Intelligence Capabilities of the US Regarding Weapons of Mass Destruction, 31 March 2005), 489–490; also available at www.wmd.gov/report/index.html.
2. E.g., USAF splits foreign intelligence and CI responsibilities between USAF Intelligence and the USAF Office of Special Investigations (AFOSI). As of 30 Sept 2005, USAF had 14,286 active-duty personnel holding intelligence Air Force specialty codes (AFSC) and only 1,283 holding the CI and special investigations AFSC. "USAF almanac 2006," *Air Force Magazine* 89(5) (May 2006): 56.
3. Joint Publication 1.02, *DOD Dictionary of Military and Associated Terms,* 8 Aug 2006, www.dtic.mil/doctrine/jel/doddict/.
4. HSPD-3, "Homeland Security Advisory System," 11 March 2002.
5. DOD, *Quadrennial Defense Review Report* (Washington DC: DOD, 6 Feb 2006), 29.
6. For information on Chinese espionage activities against the US, see Director of FBI and Director of CIA, "Report to Congress on Chinese Espionage Activities Against the US" (Washington DC, 1999); on the growing role of Chinese Special Operations Forces, see Scott J.

Henderson, "In the Shadow: Chinese Special Forces Build a 21st Century Fighting Force," *Special Warfare* 19(4) (July–Aug 2006): 30–35.

7. For a full discussion, see Colonels Qiao Lang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Panama City, Panama: Pan American Publishing, 2002).
8. DOS, *Foreign Consular Offices in the US Spring/Summer 2006* (Washington DC: Superintendent of Documents, US GPO, 4 Aug 2006), 19–23.
9. Permanent Mission of the PRC to the United Nations, www.china-un.org/eng/.
10. N. Eftimiades, *Chinese Intelligence Operations* (Annapolis, MD: Naval Institute Press, 1994), 27.
11. S. Lunev, "China's Intelligence Machine (Overseas Intelligence Activities)," *Insight on the News* 13(42) (17 Nov 1997).
12. Institute of International Education, "U.S. Sees Slowing Decline in International Student Enrollment in 2004/05," opendoors.iienetwork.org/?p=69736 (accessed 19 October 2006).
13. Federal Maritime Commission, "China Ocean Shipping Company," www.fmc.gov/reading/ChinaOceanShippingCompany.asp (accessed 1 Nov 2006).
14. T. W. Maier, "China's Military May Get US Base," *Insight on the News* 15(18) (17 May 1999): 14.
15. Air China, "English Language Homepage," www.airchina.com.cn/index.jsp (accessed 1 Nov 2006).
16. P. Brookes, "The Spies Among Us," *Heritage Foundation,* 1 June 2006, www.heritage.org/Press/Commentary/ed060106c.cfm.
17. Eftimiades, *Operations,* 17–19; Directors of FBI/CIA, "Report to Congress," 2.
18. Directors of FBI/CIA, "Report to Congress," 2.
19. Eftimiades, *Operations,* 21.
20. Directors of FBI/CIA, "Report to Congress," 1, 3.
21. P. Brookes, "Legion of Amateurs: How China Spies," *Heritage Foundation,* 31 May 2005, www.heritage.org/Press/Commentary/ed053105c.cfm; Larry M. Wortzel, "Risks and Opportunities of a Rising China" (lecture, Conference on the Asian Century for Business: A Security Challenge, Washington DC, 23 May 2006), www.heritage.org/Research/AsiaandthePacific/hl948.cfm.
22. Directors of FBI/CIA, "Report to Congress", 2–4.
23. N. Thornburgh, "The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)," *Time* 29 (Aug 2005), www.time.com/time/magazine/article/0,9171,1098961-1,00.html.
24. Directors of FBI/CIA, "Report to Congress", 1–2.
25. US Congress, House, *Report of the Select Committee on US National Security and Military/Commercial Concerns with the People's Republic of China,* 105th Cong., 2d sess., 1999, H. Report 105–851, ii, xii, xxix, xxxvi–xxxvii, 84–86, 123–130.
26. P. Brookes, "Spooks, Lies and Videotape," *Heritage Foundation,* 6 July 2004, www.heritage.org/Press/Commentary/ed070604a.cfm.
27. DOS, *Foreign Consular Offices,* viii.
28. For details of China's counterterrorism efforts and on state sponsors of terrorism, see DOS, *Country Reports on Terrorism 2005* (Washington DC: DOS Office of the Coordinator for Counterterrorism, Apr 2006), 66–67, 171–177.
29. X. G. Smith, "Special Operations Forces in the PLA and the Development of an Integral Unconventional Warfare Mission," (master's thesis, Naval Postgraduate School, June 2005), 28.
30. K. P. Ng, *Interpreting China's Military Power* (New York: Frank Cass, 2005), 128; Smith, "Special Operations Forces," 36.
31. Ng, Interpreting China's Military Power, 128.
32. Henderson, "In the Shadow," 30–35; Smith, "Special Operations Forces," 37.
33. Smith, "Special Operations Forces," 36–39.
34. A. Feickert, *US Special Operations Forces (SOF): Background and Issues for Congress* (Washington DC: Congressional Research Service, 28 Sept 2004), 1, 6.
35. J. S. Bermudez Jr., *North Korean Special Forces,* 2nd ed. (Annapolis, MD: Naval Institute Press, 1998), 1–3.
36. DOS, *Country Reports on Terrorism* 2005, 173.
37. A. H. Cordesman, *Iran's Developing Military Capabilities* (Washington DC: Center for Strategic and International Studies, 2005), 19, 46, 48–49.
38. I. Berman, *Tehran Rising* (Lanham, MD: Rowman & Littefield, 2005), 47.
39. Henderson, "In the Shadow."
40. Ng, *Interpreting China's Military Power,* 12.
41. Ibid, 25–27.
42. P. H. B. Godwin, "PLA Doctrine and Strategy: Mutual Apprehension in Sino-American Military Planning," in *The People's Liberation Army and China in Transition,* ed. S. J. Flanagan and M. E. Marti (Washington DC: National Defense University Press, 2005), 267.
43. Ng, *Interpreting China's Military Power,* 14; J. Michael Waller, "PLA Revises the Art of War," *Insight on the News* 16(8) (28 Feb 2000): 21.
44. S. J. Flanagan and M. E. Marti, "The PLA in a Changing China: An Overview," in *The People's Liberation Army and China in Transition,* ed. S. J. Flanagan and M. E. Marti (Washington DC: National Defense University Press, 2005), 5.
45. L. Linzhi, "Preemptive Strikes Crucial in Limited High Tech Wars," *Jiefangjun Bao,* 14 Feb 1996.
46. Waller, "PLA Revises the Art of War," 21–22.
47. Lang and Xiangsui, *Unrestricted Warfare,* 5, 122, 182.
48. Commission on the Intelligence Capabilities of the US, *Report to the President,* 486–490.
49. Ibid, 487.
50. For example, the FBI has sought to improve the synergy between counterterrorism and CI by placing both disciplines under a National Security Branch formed in Sept 2005; see FBI, "Statement of R. S. Mueller, Director, FBI, Before the House Appropriations Subcommittees on Science, Justice and Commerce, and Related Agencies" (14 Sept 2006). www.fbi.gov/congress/congress06/mueller091406.htm.

Vulnerability Assessment and Protection Option (VAPO) Software Tool

By: **Mr. Phillip Benshoof**, DTRA A&AS Support at Northrop Grumman IT, SYColeman

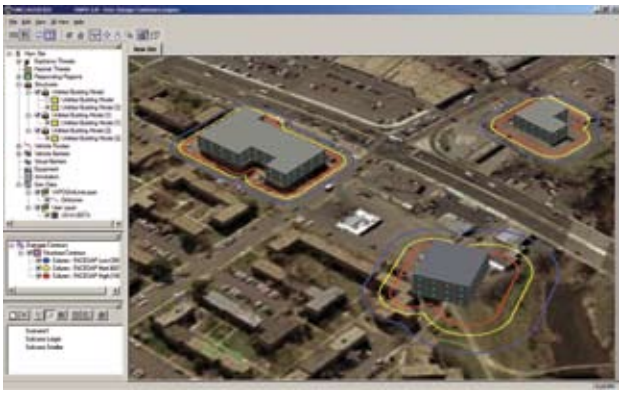
Dr. Ali Amini, Vulnerability Assessment and Protection Option (VAPO) Program Manager with the Counter WMD Technologies Directorate—Structural Dynamics Branch

Dr. Young Sohn, Branch Chief with the Counter WMD Technologies Directorate—Structural Dynamics Branch, part of the Defense Threat Reduction Agency

Joint Staff Integrated Vulnerability Assessment (JSIVA) teams have started using a new vulnerability assessment software tool for modeling terrorist threats against Department of Defense (DOD) facilities: the Vulnerability Assessment and Protection Option (VAPO). Developed by the Defense Threat Reduction Agency (DTRA) and currently in version release 2.0, VAPO is a comprehensive tool for modeling the effects of improvised explosive devices (IEDs) as well as of chemical, biological, radio-nuclear dirty bombs, mortars, and conventional weapons on structures, personnel, and equipment.

VAPO 2.0, released in October 2006 after extensive field trials in JSIVA assessments, is a user-friendly tool that provides many of the same capabilities of the Antiterrorism (AT) Planner and the Blast Effects Estimation Model (BEEM), which are used extensively by the assessment community. All three software tools can draw and view contour lines, assess a structure's vulnerability to a wide range of explosives, and view intuitive damage prediction maps in two and three dimensions (2D and 3D). VAPO, however, has several unique, state-of-the-art functions, including modeling features and structural response predictions that are more realistic and that provide more accurate vulnerability assessments.

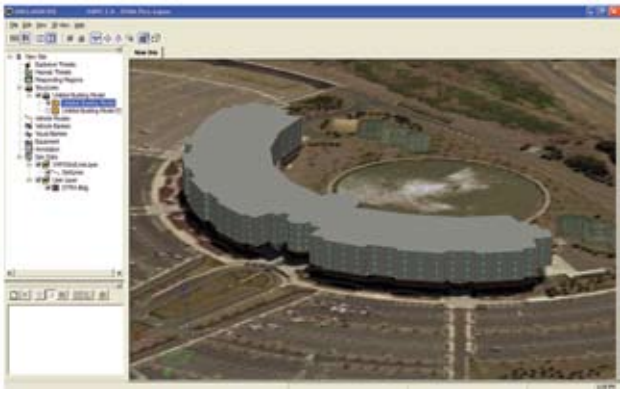
VAPO allows users to quickly model a facility, assess its vulnerability, and investigate the performance of various mitigation/protection options. Users can draw contour lines of expected structural damage around buildings or view threats in 2D or 3D representations. Minimum standoff distances—defined by DOD's Unified Facilities Criteria (UFC)—are also available and are based on user-established building occupancy and usage criteria. VAPO also includes a simple vehicle barrier-ramming calculator that determines a vehicle's end speed and ramming ability based on user-defined routes and attributes (road material, pitch, grade, etc.).



Color Contouring in 3D View

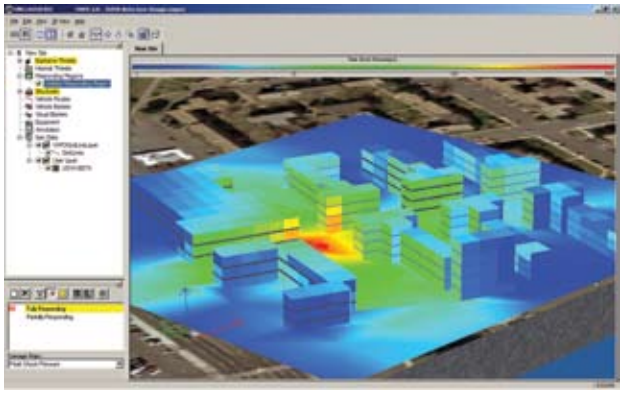
VAPO's unique automated structural designer module develops all structural components to US design standards and models them with a simple point-and-click interface. Users simply draw the outline of the building and then select the number of stories, construction materials, and type of building. Using these inputs, VAPO sizes the structural elements, such as columns, beams, and interior floor

slabs, using common gravity loads. VAPO also can model buildings with non-orthogonal (non-90-degree) wall intersections.

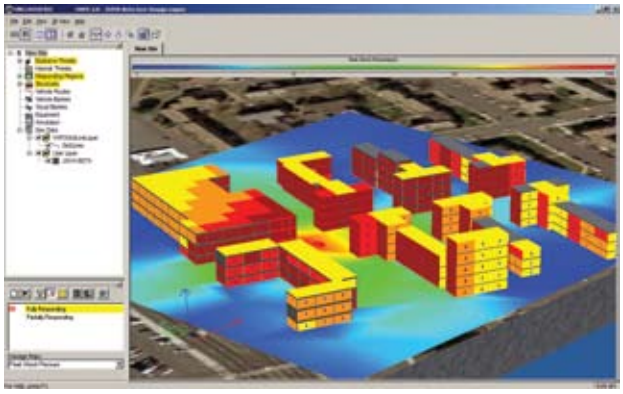


Non-orthogonal Structures

VAPO can create multiple buildings on a site and users can select the buildings that are included in blast and damage calculations, which estimate damage to selected buildings from exterior explosive threats. The blast environment calculator, Site Attack, accounts for effects of reflection and diffraction of blast pressures off of and around structures in the scenario. Urban blast pressures are represented in color and in 2D and 3D.



Site and Building Pressure Overlay



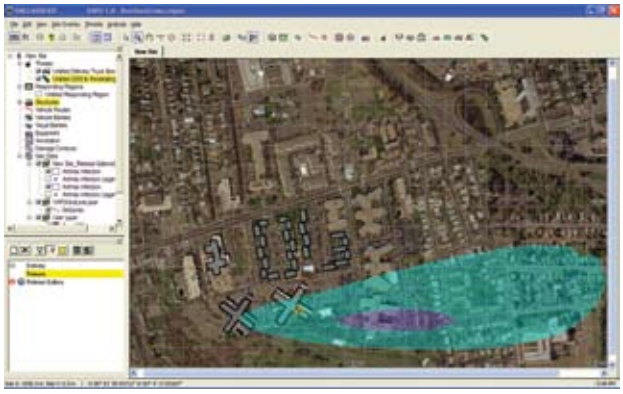
Site Pressure and Building Damage

VAPO has several unique, state-of-the-art functions, including modeling features and structural response predictions that are more realistic and that provide more accurate vulnerability assessments.

VAPO uses fast-running, physics-based algorithms to predict cratering, fragmentation, blast damage, and human injuries, and subsequent collateral effects due to the dispersion of chemical or biological agents. Calculation modules can determine glass injury from blunt trauma, such as filmed windows; penetration; internal propagation of blast pressures; percentage of occupants injured and the degrees of injury severity (linked to UFC guidelines); and the various structural retrofits that will mitigate structural damage and human injury.

Human Injury Predictions

VAPO also calculates collateral effects from chemical or biological agent releases according to DTRA's Hazard Prediction and Assessment Capability (HPAC 4.04), which is separate from VAPO. Users with an installed version of HPAC can predict HPAC collateral effects within the VAPO user interface, which graphically indicate plume area and percentage of personnel hurt within that plume using the VAPO site visualization window. VAPO incorporates extensive geographic information system-based site viewing and modeling.



HPAC Chemical/Biological Release Dispersion Predictions

DTRA, in cooperation with the US Army Corps of Engineer's Protective Design Center (USACE PDC), currently offers two training levels for VAPO users. The Level I training course teaches students the full functionality of VAPO, including capabilities, limitations, and assumptions made by the calculation models. This course shows the user how to assess and analyze a spectrum of threats against assets and how to develop threat mitigation strategies. The Level II training course teaches students how to conduct a vulnerability assessment using VAPO software, the engineering methodologies inherent in the code that predict blast environments and structural damage, and the capabilities a structural engineer can use to help develop a facility's force protection plan. Additional course information can be found at DTRA's Assessment of Catastrophic Events Center (ACECenter) website, https://acecenter.cnttr.dtra.mil/acecenter/training.cfm.

Detailed Scene

VAPO has a growing user base that includes the DTRA JSIVA and BSA Structural Engineers, DTRA 24/7 Reachback Center, National Guard Combat Support teams, Army HQ Assessment teams, USACE PDC, base/facility engineers, Antiterrorism Officers, and security personnel with several other federal agencies. VAPO 2.0 is available through DTRA's ACECenter website, https://acecenter.cnttr.dtra.mil. For more information, briefing requests, or demonstrations, please e-mail the program management team at VAPO.help@dtra.mil.

Plug It In: Integrating Department of Defense Law Enforcement Information with the Law Enforcement National Data Exchange

By Lt Col Shannon W. Caudill, Action Officer, Antiterrorism Interagency Coordination, Global War on Terrorism Branch, Joint Staff

"Information procedures should provide incentives for sharing, to restore a balance between security and shared knowledge."
— *The 9/11 Commission Report*

In the wake of the September 11, 2001, terrorist attacks, the federal government was criticized for its disjointed approach to terrorist and criminal information sharing. In July 2004, *The 9/11 Commission Report* determined that the lack of information sharing and communication system interoperability among law enforcement entities hampers investigative and response efforts and remains a gross vulnerability that terrorists could successfully exploit.

Six years later, American police departments, courts, jails, prisons, and state and federal law enforcement agencies still can't "talk" to one another. The Department of Defense (DOD) has a similar problem within its own massive bureaucracy: the lack of an interoperable law enforcement database accessible to all of its military Services and combatant commands. Each military Service currently has a separate law enforcement computer system, none of which can communicate with other Services, components, or civilian law enforcement agencies. Currently, the Army uses the Centralized Operations Police Suite (COPS), the Air Force uses the Security Forces Management Information System (SFMIS), and the Navy and Marine Corps use the Consolidated Law Enforcement Operation Center (CLEOC). Each of these programs provide the respective Service with a system for creating and maintaining police reports, incident management reports, traffic violations, and other sensitive law enforcement information.

> *"It is hard to 'break down stovepipes' when there are so many stoves that are legally and politically entitled to have cast-iron pipes of their own."*
> *— The 9/11 Commission Report*

Each military department's law enforcement system was designed to support the Defense Incident-Based Reporting System (DIBRS), which was required by DOD in 1996. DIBRS supports the National Incident-Based Reporting System (NIBRS) requirements, which were mandated by the Uniform Federal Crime Reporting Act of 1988, Victim's Rights and Restitution Act of 1990, and the Brady Handgun Violence Prevention Act of 1994. DIBRS is the DOD repository for statistical data on criminal offenses and other concerns, including suicide, fraternization, drug abuse, sexual assault, and sexual harassment—all of which are congressional high-interest issues. DIBRS aimed to provide DOD crime statistics to the Department of

Justice (DOJ) and to Congress, but was not designed to interface between the Services or to improve information sharing between DOD law enforcement agencies.

The national law enforcement community has invested billions of dollars in database management and stores records in many unaligned formats and technology platforms. To answer this problem, DOJ and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division set the goal of creating a standard law enforcement operating system called the Law Enforcement National Data Exchange Environment (N-DEx).

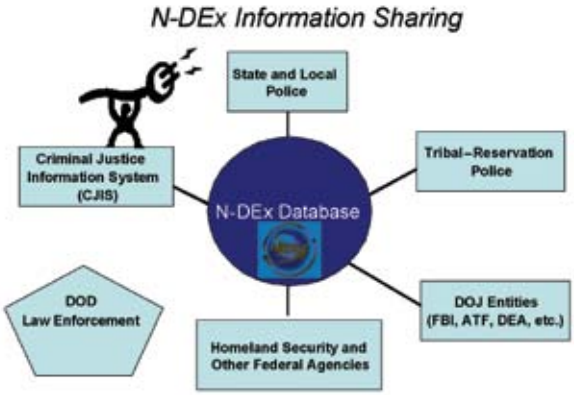
DOD's DIBRS is positioned to share law enforcement information because its core data elements and those of NIBRS form a major subset of the core data elements of N-DEx. In 2004, DOD participated in a variety of DOJ-sponsored forums and working groups designed to foster the development of N-DEx. DOD, represented by the Office of the Under Secretary of Defense (Personnel and Readiness) Program Integration Office, chaired the Law Enforcement N-DEx Federal Working Group. DOD also sits on the N-DEx Project Development Council and has stakeholder representation through its seats on the CJIS Advisory Policy Board Federal Working Group.

N-DEx enables timely and accurate law enforcement information sharing across jurisdictional boundaries and provides an advanced investigative tool to fight crime and terrorism. This system promises to provide nationwide connectivity to local, state, tribal, and federal law enforcement systems, allowing users to search, link, analyze, and share information on a national basis. N-DEx will allow participating agencies to detect critical relationships between key evidence and information and enable users to link data across jurisdictions. The ability to mine the data system for relevant facts and information will facilitate unprecedented law enforcement agency collaboration. For example, when an N-DEx user searches for a person's name, the system will automatically provide relevant links to information throughout the N-DEx user database and correlate "people, places, and things." All law enforcement information shared through N-DEx will originate from local, state, tribal and federal systems and include incident and arrest reports, case files, booking reports, incarceration records, criminal histories, and other pertinent data.

In February 2007, the FBI awarded the N-DEx development contract to Raytheon Inc. The initial, incremental deployment of N-DEx is scheduled for February 2008 and will offer an estimated 50,000 users basic search engine and correlation capabilities. In February 2009, Increment II is projected to double the amount of users and implement advanced research and analysis features. Increment III, with a user population of 200,000, will be a complete system with fully advanced analysis tools linking databases to a wide range of criminal justice entities, including probation and parole agencies.

"The development and deployment of N-DEx will provide nationwide capability to share information derived from incident, arrest and event reports. This will expedite coordination across law enforcement so that we can remain one step ahead of the criminals and terrorists despite jurisdictional boundaries."
— Zalmai Azmi, FBI Chief Information Officer

Importantly, the ownership of data shared through N-DEx remains the property of the law enforcement agency that provided it, which will allow criminal justice entities to protect critical information and privacy according to local terms and to applicable laws. Although law enforcement will be the primary focus of N-DEx, future versions will incorporate the larger criminal justice community like courts, probation agencies, parole boards, and prisons. N-DEx will offer a range of database management options, from computer-based automated records management systems to paper-based systems.



N-DEx Information Sharing Diagram

With N-DEx, DOD law enforcement information technology management will advance by leaps and bounds. N-DEx ensures a common interface and operating system for law enforcement database management and offers a "plug and play" capability with DOJ and local law enforcement, which—if fully exploited—will provide a common operating picture across the spectrum of military law enforcement data needs. By migrating to a common law enforcement database, a new N-DEx-based system will facilitate law and order and antiterrorism operations in the combatant commander's area of operation and provide the warfighter with a common sight picture on potential criminal and terrorist operations across the theater.

"We will continue to improve law enforcement capability, including greater and more effective collection and reporting of intelligence, without encroaching on the privacy and civil liberties of Americans, to interdict terrorists before they strike the Homeland."

— *The White House, 9/11 Five Years Later: Successes and Challenges, September 2006*

The end result of the N-DEx enterprise promises to be a fully networked national law enforcement system that will improve homeland security and the fight against terrorism. DOD law enforcement also will become more relevant and efficient by linking into the N-DEx network. The first DOD agency to participate in N-DEx will be the Air Force Office of Special Investigations (AFOSI), which is completing the final preparation of its system, Investigative Information Management System (I2MS), and will begin N-DEx data submissions by the end of July 2007. AFOSI's pilot program will give DOD a clearer picture of system and training requirements, and provide a starting point for DOD law enforcement integration into N-DEx.

To quote General Peter Pace, Chairman of the Joint Chiefs of Staff, "Information, perception, and how and what we communicate are every bit as critical as the application of traditional kinetic effects." DOD's law enforcement data transformation is critical to mission success in the Global War on Terror. N-DEx provides an unparalleled opportunity to modernize DOD law enforcement information systems and fully integrate them into the larger, national law enforcement network.

For more information on N-DEx, go to: http://www.fbi.gov/hq/cjisd/ndex/ndex_home.htm.

Our Own Worst Enemy: Why Our Misguided Reactions to 9/11 Might Be America's Greatest Threat

By Randall J. Larsen, former chairman, Department of Military Strategy and Operations at the National War College

PART 2

This is the second part of a two-part article originally written in July 2005. The first part, which appeared in our last issue, addressed the shortcomings of America's response to the terrorist threat and put forth a strategy for containing that threat and deciding where to concentrate our efforts. Part 2 discusses various elements that will support these efforts, such as executive education (teaching our leaders how to think), information systems (knowing what we know), and both protecting and utilizing corporate America in the Global War on Terror.

Executive Education: Teaching Leaders How To Think

One of the primary reasons for the success of the US military during the past quarter-century has been an aggressive and unflagging commitment to executive education. This is far different from training. The Department of Defense spends billions of dollars each year on training: training people to drive tanks, fly airplanes, and shoot M-16s. A much smaller, but equally important investment is made in executive education: teaching leaders how to think (as opposed to what to think).

This executive education takes place throughout an officer's career, and the final step in this program is called senior service school. During my final military assignment, I served as the Chairman of the Department of Military Strategy and Operations at the National War College. War is certainly a major topic at the National War College; however, it goes far beyond the ideas of Karl von Clausewitz. From the modern-day American perspective, the purpose of war is to build a better peace. Therefore, when the students at the National War College look at World War II, it is from a perspective on how it changed the international structure: from the creation of the United Nations, to the Bretton-Woods Agreements that led to the International Monetary Fund, to the development of nuclear weapons that changed the entire international security equation.

The students, a highly select group that are destined for senior leadership positions in the military, intelligence community, and other executive branch agencies, learn how to think about national security. Because of bureaucratic politics, it still says National War College on their diplomas, but, in reality, they receive a master's degree in strategic thinking. This is certainly one of the reasons why the graduates go on to highly successful careers in government and are also highly successful in the corporate world following retirement from the military. They become strategic thinkers.

This sort of executive education is what is missing in homeland security, both in the public and private sectors.

And, this sort of executive education is needed not only for leaders who will respond in a crisis, but also for leaders who will decide how America should prepare. What strategy should we adopt? Where should we be spending funds for homeland security, both in the public and private sectors? What should a CEO do to protect business processes and employees? How do leaders ensure they will produce a proper return on investment? How can we expect our leaders to make the right decisions if they are not properly educated for the task?

This lack of education and understanding is the single greatest reason for America's misguided reactions to 9/11. There are two different requirements for homeland security education: long-term (traditional education in universities) and short-term, executive level education. If we look back a few generations, we can see two other times when national security interests initiated education programs that served not only the immediate security needs, but also played major roles in the economic development of this nation.

In 1862, President Lincoln signed the Morrill Act, which created the land-grant schools. The legislation had failed to make it through Congress on previous occasions, but the addition of a requirement for military training (in response to the lack of qualified officers for the Union Army) guaranteed passage. The land-grant schools were directed to focus their efforts on the two great engines of the American economy, agriculture and engineering, and they provided three services: teaching, research, and extension programs. These three key public services still serve as the core of land-grant universities.

The vast majority of junior colleges, colleges, and universities have all developed "homeland security programs." However, most are little more than training programs for first responders. Not that these are not important programs; they are, but they fall into the category of training, not education. Training programs teach people how to do things based on years of accumulated experience: fight fires, give first aid, use a computer program or other piece of equipment. Education programs teach people how to think.

Here is one example. Law enforcement officers spend many hours a year in training programs. Several new training programs have been designed for homeland security such as responding to chemical and radiological attacks. They are based on years of experience from military training programs. If this event happens, here is a checklist of what you must do.

Education programs are quite different. I developed a one-day education program for the Washington State Sheriffs and Police Chiefs Association. During the morning session, the participants were directed to plan a terrorist attack on their own communities.

Lack of education and understanding is the single greatest reason for America's misguided reactions to 9/11.

What began as required classes on military-subjects during the Civil War evolved into the Reserve Officer Training Corps (ROTC) in 1916. This program provided thousands of officers for service in World War I. The ROTC program was further expanded in 1920. This investment paid great dividends when America's armed forces grew to 12 million during World War II.

In 1958, in response to the launch of Sputnik, the National Defense Education Program (NDEP) was created, and, once again, education was a critical element of America's response to a national security challenge. NDEP was of great value to America's success in the Cold War, but also to America's economic success. It is not difficult to link America's leadership position in technology and success in the global marketplace back to the NDEP investment in education.

With these two programs as benchmarks, America must now look to its universities to prepare future and current leaders for the security challenges of the 21st century. Training must begin at the undergraduate level and continue through the graduate and post-graduate levels, but it must also include short courses for leaders who have already completed their formal education, and even shorter programs for busy executives.

They were given a political objective (cause serious economic, social, and psychological disruption) and told what resources they had at their disposal (numbers of terrorists, types of weapons, and other resources). The senior law enforcement officers were at first hesitant, but as they discovered how easy it was to plan and conduct such attacks, they began to have a new perspective on the security of their communities.

After lunch, they were told to respond to the coordinated suicide attacks on local shopping malls that had been conducted on the Friday after Thanksgiving. The officers suddenly found themselves in new territory. There were no checklists, and they had little experience in this type of scenario. For their entire careers, they had been focused on investigating crimes, pursuing and apprehending the perpetrators, and moving them through the judicial system.

In this case, the perpetrators were all dead. The mission of the law enforcement official was to convince the citizens of their communities that it was safe to go back to the shopping malls. If the shoppers did not go back, it would cause enormous economic disruptions—not only to the local business owners, but to local tax revenues. This was a new mission for law enforcement officials.

When it comes to first aid, crime scene investigation, and weapons training, there are right and wrong

answers. These right and wrong answers are based on years of experience. The purpose of this one-day workshop was not to teach the answers, but to teach the senior officers what questions they should be asking. This is education. Today, there is a significant amount of federal money being spent on homeland security training, but very little on homeland security education. That must change.

Several universities are working to develop undergraduate and graduate education programs in homeland security. Texas A&M (a land-grant school) is designing a program that will provide the same type of education for homeland security leaders that the National War College has provided national security leaders for several decades. We need to leverage the successes of the past to develop this new academic discipline.

Finally, homeland security should not be viewed as just a course or a department in a university. It must be integrated throughout the various colleges and curricula: science, economics, law, medicine and public health, engineering, and business. Homeland security is a fact of life in the 21st century. It will influence all that we do. A large-scale investment in homeland security education will allow America to control the high ground of security in the 21st century.

Information Systems

Information is the weapon that terrorists fear most. We must use it wisely, and in a manner consistent with the value we place on privacy and civil liberties. Information is an area where we have a huge asymmetric advantage over the terrorists. Unfortunately, America has a poor track record in using this advantage. Here are just a few recent examples:

- On 9/11, the State Department had fewer than 80 employees who were fluent in Arabic—despite the fact the State Department and the intelligence community knew that Islamic terrorists were a serious threat to our homeland and interests abroad. This lack of "area specialists" was not limited to one agency. It was common across the interagency community.
- Prior to 9/11, the Central Intelligence Agency discovered a way to identify forged passports used by al Qaeda, but they did not share this information with those US officials who examine the passports of people entering the United States. At least 7 of the 19 hijackers from 9/11 had forged passports.
- Prior to 9/11, the chief of the al Qaeda analysis team at CIA called the National Security Agency (which collects intelligence information through electronic intercepts of radios, telephones, the Internet, etc.—known as "SIGINT") and asked to receive the raw data from these intercepts rather than just the NSA analysis. He was told, "We don't provide that information outside of this agency."
- In July 2001, a Florida state trooper stopped Mohammad Atta (operational leader of the 9/11 attacks) for a traffic violation. The trooper queried the National Crime Information Center for any information on Atta. None appeared, and he was released with just a citation for having an expired driver's license. At that time, Atta was listed in numerous federal government databases for suspicious behavior.

Information is a broad term, so, first, let us agree on a definition for this discussion. When talking about homeland security, information includes intelligence (from the most highly classified levels to open source, such as newspapers and radio broadcasts in foreign countries), knowledge about activities in other government agencies (left hand not knowing what the right hand is doing syndrome), and government and private sector databases other than those in the intelligence community.

Let us also agree on realistic expectations. Information is a highly useful tool for defending our homeland, but we should never believe that with enough investment in information, we could prevent all or even the majority of attacks on our homeland. Military intelligence officers like to point out that one's opponent in a chess game has an extraordinary amount of information. All pieces are in clear view, and the capabilities of each piece are well defined by the rules of the game. Nevertheless, there is an extraordinary amount of surprise and deception in chess. In the realm of homeland security, we can see only a small portion of the "chessboard" and the opponent often plays by different rules.

This explanation is not meant to provide an excuse to the intelligence community for failing to predict or prevent 9/11. Actually, the intelligence community did predict 9/11. As early as 1998, the director of the Central Intelligence Agency, in open congressional hearings, stated that al Qaeda was targeting America. Nevertheless, there is considerable room for improvement.

First, we must improve how we collect and analyze intelligence information. The National Intelligence Reform Act, passed earlier this year, is a great step forward, with the potential to significantly improve our collection and analysis efforts. The new Director of National Intelligence, John Negroponte, and his deputy, General Mike Hayden, will have the opportunity to eliminate obstacles, better coordinate efforts, and build an intelligence community to meet the challenges of the 21st century. [*Editor's note: the current director is Mike McConnell.*] Their initial actions, which have included breaking a few iron rice bowls, are exactly what is needed. They should not be timid or walk softly in their vital mission of transforming

an intelligence community that is still primarily organized, trained, and equipped for the Cold War.

Second, the Federal Government needs a 21st-century information system. Today, many agencies "do not know what they know." The most egregious single example is the Federal Bureau of Investigation. The previous director, Louis Freeh, did not like computers. In fact, on his first day in office in 1993, he told his staff to remove the computer from his desk. That became the corporate culture. While the rest of the world was rapidly moving into the Information Age, the FBI was continuing to handle information in much the same fashion as in the days of J. Edgar Hoover. Shortly after 9/11, the FBI signed a contract to build an electronic case file system. With such a

The federal government needs a 21st-century information system. Today, many agencies "do not know what they know."

system, if a special agent in Arizona filed a report about Middle Eastern young men paying cash for flight training, an analyst at headquarters could search the database for reports of other such activity. Unfortunately, after spending $170 million trying to build such a system, the FBI shut down the project earlier this year and declared it a failure. It is hard for me to imagine how a nation that leads the world in the technological revolution would allow the FBI to fail in such an important endeavor. Today, the FBI still doesn't know what it knows. It has an incredible amount of valuable information, but no means for electronic search and analysis.

This same problem exists within the interagency community. According to one of America's most experienced biodefense experts, Dr. Robert Kadlec,[1] there is no database in existence to identify and track federally funded programs in biodefense. In other words, the Departments of Defense, Health and Human Services, and even Homeland Security often spend millions on research programs without coordinating their efforts. There are scientists working on similar programs, funded by different agencies, who are not aware of others doing similar work. This is a case of failing to use 21st-century information technology to our best advantage.

The third area of information that could provide us with a superb return on investment has to do with the linking of public and private sector databases. This is an area that causes great concern to many in the civil liberties and privacy communities. Their worries can be fully understood. However, there are means to approach this issue that will provide the protection needed to meet our cultural and legal standards. Much work has been accomplished by think tanks and other not-for-profits on how we can use information technology without sacrificing our privacy. The Potomac Institute's work on the Project Guardian is one to be commended. They have designed a system that allows our incredible information technology to outwit the enemy while at the same time involving all three branches of government in providing the oversight necessary to protect our privacy.

The technologies exist today that would allow local, state, and federal law enforcement organizations, plus intelligence agencies, to pass information to a common data hub for national level compilation and analysis. The hub would be the National Counterterrorism Center, which also needs the capability to provide processed intelligence and information to local, state, and federal law enforcement agencies. Information technologies exist today that would have caught at least 11 of the 19 hijackers before they boarded their airplanes on 9/11. This leads to the fourth, and, perhaps, most controversial, subject under the banner of information—personal identification.

Today, 15 European nations have a form of nationally standardized identification. The United Kingdom, after much debate, has recently decided to begin such a program. Some would say that we already have one in the United States—our state-issued driver's license. We all use it every time we transit an airport. The only problem is that it does not provide us with an effective antiterrorism system. We have all heard the stories about the 9/11 hijackers—that seven had Virginia drivers' licenses, and none lived in Virginia. There are some states with laws that authorize the issuance of drivers' licenses to people who are known to be illegal aliens (Michigan requires it). We all know that any reasonably intelligent college student understands how to use the Internet to get a photo ID card that "proves" he or she is 21. Al Qaeda certainly knows how.

We are in the process of spending billions of dollars on the US-VISIT program that was designed to deter

or capture terrorists entering our country. If and when the system becomes highly effective, the terrorists will stop using our ports of entry and begin crossing our 7,500 miles of unguarded borders and 95,000 miles of shoreline. Remember, they are a thinking enemy. When we close and lock one door, they will move to another. We can spend ourselves into bankruptcy by staying just one step behind them.

It is understandable why many Americans worry about the creation of a national identity card. I have serious concerns myself. Nevertheless, we have reached a point in time where the lack of national identity cards may be a greater threat to your family than the creation of such a system. Senator Lamar Alexander (R-Tennessee) recently changed his mind. Twenty years ago, while serving as the governor of Tennessee, he vetoed a bill requiring photos on drivers' licenses. He thought it was an unreasonable breach of privacy. Today, Senator Alexander is calling for national identity cards—with photos and biometrics.

The reason he and many others have changed their minds is that the creation of national identity cards is something akin to medical procedures—they all have risks; but when the risk of inaction becomes greater than the risk of action, action becomes the better choice.

Nevertheless, many Americans are not ready for a national identity system. I am one of them. However, if we experience several major attacks, larger and more deadly than 9/11, the American people may change their attitudes on this subject. A poll taken shortly after 9/11 stated that 70 percent of Americans favored a national identity system.

We must take action now, before the next attack. Our analyses and decisions are likely to be far better than when we are in shock following a large-scale attack. First, we should conduct a comprehensive, nonpartisan study to examine the critical issues of a national identity system. Second, we should consider quickly moving forward with a novel concept for identification—a privately issued, government-recognized travelers' ID card. This would be a voluntary program.

Congress should form a bipartisan commission to do a one-year study on a national identity system. The commission should focus on four questions:

1. Does an organization and system exist that can ensure identification credentials are properly issued?
2. Does the technology exist to create a means of identification that cannot be altered or counterfeited?
3. Can we build a system that is affordable?
4. Does the American public feel secure that such a system would protect their privacy?

Today, the answers are no, yes, yes, no. The purpose of the study would be to determine if it is technologically and politically feasible to get four "yeses." The American public may not support a national identity system until we can obtain four yeses. Is this possible? Absolutely, but a lot of work is needed. The first question (ensuring credentials are properly issued) will be the most difficult to resolve. It will require that we first answer other questions, many involving immigration and illegal aliens. The last question (privacy) is the one that causes many to object, but, in reality, it may not be as difficult as you think. Much work has been accomplished in this area. Technology will allow the creation of a system that would make the threat of "big brother" far less than most would expect.

Perhaps we should include a fifth question: Would such a system make us more secure? The answer is yes. There is no way to effectively control 7,500 miles of borders and 95,000 miles of shoreline. If we spend billions making it virtually impossible for known terrorists to enter the United States through our sea, air, and land ports, they will begin crossing our borders in the same way the economic refugees and migrant workers from Mexico and Central America have done for decades. And even though some members of Congress want to build impregnable borders with physical and electronic barriers, you must understand such an initiative would be no more effective in protecting our homeland today than the Maginot Line was in protecting France in 1940. It would waste valuable resources and leave us no more secure.

There is no way to effectively control 7,500 miles of borders and 95,000 miles of shoreline.

On May 11, 2005, the President signed the Real ID Act, which establishes national standards for state-issued drivers' licenses. This is a step in the right direction; however, it will be 2008 until it takes effect, and even then, states are not required to comply. The good news is the Real ID Act may be a step toward improving the reliability of identification, and it will focus efforts on the first question (ensuring credentials are properly issued). The bad news is that 2008 may be too late. Perhaps we should look to the private sector for quicker solutions.

On June 9, 2005, the House Committee on Homeland Security held its first hearing to discuss the concept of privately issued, government-recognized travelers' IDs. If frequent travelers want to pay several hundred dollars for such a card, and don't mind being fingerprinted, iris scanned, and background checked, then TSA would not have to act as if their next trip through an airport is their first. The card, similar to a pilot program run by TSA called "Registered Traveler," would allow TSA to focus its efforts on those who had not agreed to background checks and biometric scans. This strategy comes right out of the textbook on risk management. It would allow TSA personnel to spend more time focusing on those who might actually have nefarious plans. This is a winning strategy for all homeland security programs—focus resources where the threat is the highest!

These are but a few examples of how 21st-century information systems can serve as our most effective weapon in the War on Terror. Corporate America can provide the technology—that is not the challenge. The challenge is breaking away from 20th-century paradigms, bureaucratic politics, and stovepipes. We must also develop an oversight system to ensure Americans that their privacy and civil liberties will be protected just as aggressively as we seek to detect, deter, and defeat the terrorists.

The Role of Corporate Leadership

Several CEOs have asked me why they should worry about homeland security. "Isn't that the government's job?" Whenever I hear this question, the words of Leon Trotsky come to mind, "You may not be interested in war, but war is interested in you." Trotsky's dictum also applies to 21st-century terrorism.

Businesses have become the prime targets of international terrorists. According to the US State Department, between 1996 and 2003, there were 2,479 terrorists attacks worldwide. Businesses were the targets for 2,074 of these attacks (diplomatic facilities 230, government 123, and military 52). General Electric Corporation executives did not soon forget the 9/11 attacks.

Many of the 19 hijackers walked through screening devices made by GE. (The box cutters were not illegal at that time.) All four engines on the two airplanes that hit the World Trade Center towers were built by GE. Both airplanes were owned by GE and leased to United and American Airlines. GE was a secondary insurer of World Trade Center towers 1, 2, and 7, and GE owns NBC, which had no advertising revenue for several days following 9/11. That was Jeff Immelt's first week as CEO of General Electric.

On December 26, 2001, Osama bin Laden said, "If their economy ends, they will busy themselves away from the enslavement of oppressed people. It is important to concentrate on the destruction of the American economy." Therefore, corporate America must be resilient to attack. The top priority should be to ensure that employees and business processes are protected. But what does this mean?

One year after 9/11, the Council on Competitiveness did a survey of US corporate CEOs. They asked if major investments had been made in security. The answer—less than 10 percent of CEOs said they had made significant investments. Why? No one could provide them with a sound cost-benefit analysis. In discussions with various corporate security officers, I find this is the most common challenge security managers face. How does one convince a CEO that investments in security against terrorist activity will receive strong support from shareholders?

Some say it will provide lower insurance rates, yet there is little evidence to support this claim. Insurance rates are based on historical data. According to a recent article in *Business Week,* companies that provide auto insurance have increased their tiers of rates for drivers from 3 (preferred, standard, and nonstandard) to more than 300. This has been possible because of the insurance companies' ability to build enormous databases on different categories of risk. In the past it was mature drivers with no traffic violations or accidents, drivers with a few (nonserious) events, and 17-year-old boys with speeding tickets on their records. The insurance companies' ability to develop hundreds of different risk categories (or tiers, as they call them) is a benefit to both the companies and the policyholders. Unfortunately, there is no such data on the terrorism risk.

Another issue that causes problems for corporate leaders has been superbly documented by Stephen Flynn, a transportation security expert at the Council on Foreign Relations. He demonstrates how an investment in security could put a company at a competitive disadvantage. For instance, if there are 10 companies operating in a seaport, and only company X chooses to invest in increased security against terrorist activities, company X will have increased operating costs, but, in reality, no increased security. A chain is only as strong as its weakest link, so the seaport will remain just as vulnerable as it was before the investment by company X.

On December 26, 2001, Osama bin Laden said, "If their economy ends, they will busy themselves away from the enslavement of oppressed people. It is important to concentrate on the destruction of the American economy." Therefore, corporate America must be resilient to attack. The top priority should be to ensure that employees and business processes are protected.

If no attack occurs, company X will realize a competitive disadvantage because of increased operating costs. If an attack does occur at one of the other nine companies within the port, the government is likely to step in and demand "new port security measures." These measures may not be the same as those in which company X has already invested. Therefore, company X would have to make further investments. As a stockholder of company X, I might question the original investment. This is the dilemma CEOs now face. What to do?

This is not just a hypothetical issue. During a hearing before the Senate Homeland Security and Governmental Affairs Committee on June 16, 2005, Robert Stephan, Homeland Security's acting Undersecretary for Information Analysis and Infrastructure Protection, stated that the chemical industry has voluntarily spent $2 billion on security since September 11, 2001. However, he also noted that 20 percent of the nation's 3,400 chemical plants have "sidestepped voluntary standards." (This, of course, provides them a competitive advantage.) Congress is now considering mandatory standards. But what if these standards are different from those in which many companies have already invested? What are corporate leaders to do?

The first step is to ensure that corporate leaders are asking the right questions. This leads us back to education. Just as we have entered a new national security environment, we have also entered a new business environment. Sarbanes-Oxley, the accounting reform law, has caused CEOs to ask a lot more questions about financial matters. Likewise, the threat to our homeland should cause CEOs to ask new questions, not just of their security managers, but from all personnel on the leadership team.

Here are two brief examples from the auto industry. One company recently hired a major consulting firm to conduct a homeland security exercise for the executive leadership team. During the exercise, terrorists destroyed the bridge between Windsor, Canada, and Detroit, Michigan. This 7,500-foot bridge carries 25 percent of all merchandise trade between the United States and Canada. More than 12,000 trucks cross the bridge each day, many of which move auto parts both ways across this international border. When provided this challenge, the vice president for operations stated, "Well . . . I guess the Army Corps of Engineers will have to build a pontoon bridge. I assume they could do this in a few days."

While it is a good sign that this corporation conducted this exercise to examine the threats to its business processes, it was also obvious that they previously had not seriously considered this type of threat. The 7,800-foot pontoon bridge on the Hood Canal in Washington State took three years to build. Combat-style pontoon bridges can be built considerably quicker, but require tugboats to hold them in place against the current, and would have great difficulty carrying even one-tenth of the traffic that uses the Ambassador Bridge each day.

Another US auto manufacturer has an assembly plant that now requires all parts suppliers to be located within 500 miles, and none can be in Canada. Following the reactions to 9/11, this company did not want its production to be dependent on the ability to quickly move across international borders. This requirement ensures the company will better protect its business process from transportation disruptions, but it also ensures higher costs.

In both cases one must ask, did the leadership team ask the right questions? In my opinion, the answer is no.

One thing we know for sure, there will be no quick, easy, or inexpensive answers to these questions. America's corporations were designed and built to operate in a secure environment. This may not always be the case. Many of the changes required will be long-term initiatives. Including security in new designs of facilities and processes is far less expensive than refurbishing existing facilities and processes. Security needs to become as intrinsic to corporate America as safety and quality.

Transportation seems to be one of the most vulnerable segments of the commercial sector. Last year, I was the keynote speaker at the North American Cargo Security Conference in Washington, DC. During the question and answer session, a well-known security consultant asked me this question: "Don't you agree that there is a high probability that after the next major attack, the government will likely overreact and cause more damage to our economy than the terrorists?"

I said: "No. I disagree. It is not a high probability—it is a sure thing."

So, what does this mean to corporate executives? First, there will be no excuse for being surprised when the next attack occurs, or when the government overreacts. Second, this means corporate America must prepare. Using industry associations, corporations should have plans that have been thoroughly examined—perhaps even tested in a pilot project—and then placed on the shelf. When a major event occurs that will require some sort of immediate action by the government, industry associations can then step forward to offer assistance.

With proper coordination, America's corporations, large and small, could play a major role in responding to disasters.

We all know that the government will need to take action to assure the American people and the markets. If industry associations provide the government with a plan that demonstrates positive action (improving security), without destroying or seriously harming industry, Congress and the administration are likely to endorse the idea. They may even take credit for a good idea. (Let them.) Corporate America's reward will be avoiding serious disruption to business processes.

If you think I am exaggerating the potential damage of government overreaction, consider this. One year after 9/11, I sat in on a meeting with a very senior Transportation Department official. He said that if a weapon of mass destruction, such as a radiological dispersal device, went off in a seaport, he would shut down all ports until he could asssure the President that all containers were secure. (Seventeen thousand containers move through US seaports each day. It takes four people, four hours to search one container.) The room went silent, except for the sound of 20 jaws hitting the table. The economic consequence of such action for corporate America and the economy (US and global) is hard to fathom.

The best homeland security investments for corporations are the following: executive education; the creation and implementation of industrywide security standards; the development of essential policies tailored to the particular corporation or entity; and table-top or simulation programs that "test" business continuity, consequence management, and other contingency programs. Ray Humphrey, former president of both the American Society for Industrial Security (ASIS-International) and the International Security Management Association (ISMA) agrees with this assessment. "If you do not properly prepare, you will discover that the US government will not necessarily be available during the early phases of the crisis; you will learn that a crisis is not the time to be engaged in relationship building; and you will definitely find that prior planning and simulation exercises would have provided a wealth of 'lessons learned.' Lack of preparation may well be a greater threat to the corporation than al Qaeda."

Another role that corporate America can play in homeland security is in the area of public service. My favorite TV commercial is the one produced by Miller Brewing Company. The narrator talks about how Miller helps local communities respond following natural disasters. Bottlers in a local community just outside the disaster area immediately stop bottling beer, and instead put water into their bottles. Miller then ships the bottles to the disaster areas. At the end of the commercial, a relief worker (who looks as if he has been awake for about a week) thanks Miller for its public service. He then says, "But guys, every once in awhile, you could put beer in a few of the bottles you send us."

Not only does Miller get great credit for public service, it is great marketing. When I walk down the beer aisle at my grocery store, I always think of that commercial when I see the Miller brand.

The fact is, most corporations want to help following a major crisis. Unfortunately, their help is not always well coordinated. By the late afternoon of 9/11, many of the local businesses realized that the recovery effort at the Pentagon was going to require a 24-hour effort for several days. These local business leaders wanted to do something to help. Many of the fast-food outlets in the local area sent free food for the first responders. It was a great gesture, but most of the food was wasted. The effort was not coordinated.

With proper coordination, America's corporations, large and small, could play a major role in responding to disasters. Under the newly created National Response Plan, a Joint Operations Center (JOC) is established whenever there is a major disaster, man-made or natural. This is a central command center where federal, state, and local officials coordinate efforts. To best support the government JOC, the private sector needs to have its own JOC. With all of the volunteer corporations working together, they could avoid the waste of the 9/11 response at the Pentagon and provide extraordinary assistance to the response effort. When the government JOC determines it needs food, transportation, or communications

assistance, only one phone call would be necessary—to the private JOC. The corporations could then coordinate their efforts. This type of private-public partnership would play a critical role in response efforts.

Perhaps the most important role corporate America will play in defending our homeland will be in the technologies and services provided to federal, state, and local governments. However, these corporations, large and small, need the protection Congress intended when it passed the SAFETY Act (Support Anti-Terrorism by Fostering Effective Technologies Act of 2002). The SAFETY Act was designed to protect corporations from lawsuits involving newly developed systems and technologies to provide us an advantage over the enemy. According to a Department of Homeland Security press release:

> . . . the Act provides a number of benefits to both companies and the American public. Companies investing in the development and deployment of qualified antiterrorism technologies will be provided with unique protections that will minimize their risks should they be sued in connection with a terrorist attack. Without the Act, many companies may not invest in potential life-saving technologies to protect Americans.

The Secretary of Homeland Security has been given the authority to determine whether an antiterrorism technology is considered qualified through two mechanisms designed to limit liability: "designation" and "approval." For a company's antiterrorism technology to receive a "designation," they must be evaluated against a list of specific criteria. To obtain an "approval," the technology also must meet additional specifications requiring that the technology performs as intended, conforms to the seller's specifications, and is safe for use as intended.

Once this designation/approval is established, companies using SAFETY Act protections will have their cases heard in federal court versus state court venues. In addition, the protections create a "government contractor defense" in cases where it would not otherwise exist.

The SAFETY Act provides a critical framework for encouraging the entrepreneur and the established manufacturer to develop and deploy the technologies necessary to protect America from terrorist attacks.

For instance, if a company developed a new sensor that was far better at detecting explosive material than current technologies, we would want to rapidly deploy that technology. However, if this technology succeeded 99.99 percent of the time—a huge improvement over current technology—but failed .01 percent of the time, should the corporation be liable if an explosive device made it through this screening system? Should the families of those killed or injured in an attack be able to sue the corporation? Congress emphatically said, "No."

However, last year a CEO of a $20+ billion defense contractor told me that his company had submitted a bid to the Department of Homeland Security with the caveat that the company would receive SAFETY Act protection for this contract. The Department of Homeland Security returned the bid. The department stated that this was a two-step process—one office in the department would evaluate the bid and another office would determine if it would receive protection under the SAFETY Act. The CEO refused to resubmit the bid without the caveat. He stated, "I can't bet my corporation on the possibility of receiving SAFETY Act approval after the contract has been awarded."

To best leverage the resources of American technological power, the Department of Homeland Security needs to improve the process that Congress intended when it passed the SAFETY Act. In theory, it is a great idea, but as they say, the devil is in the details. This is one detail that requires high priority attention from the Department of Homeland Security.

Corporate America played a vital role in winning the Cold War. It provided the technologies and industrial might that allowed containment to succeed. In the 21st century, corporate America will play that same role, but it also will play new roles, such as providing public service assistance during periods of crisis. However, corporate America must also understand that it needs to protect its own interests—from terrorists, tort lawyers, and government overreaction.

Conclusion

America must have a comprehensive strategy for defending our homeland in the 21st century. This strategy will drive our spending priorities and regulatory initiatives. While there are many spending priorities, the top priorities for homeland security are nuclear and biological defense, education programs, and information systems.

We must keep our perspective, we must not overreact. The British government and its citizens displayed great character and courage in their response to the July 2005 bombings in London. America must follow their lead. America can survive a car bomb or two. America can survive an attack on a train, a shopping mall, a chemical plant, or even another attack with an airplane. On the other hand, attacks with nuclear and biological weapons have the potential to radically change our political, social, and economic foundations. They are in a class by themselves and must be our top priority.

Members of Congress have many pressures to provide homeland security funds for a wide variety of threats. Every fire department, police department, sheriff's department, emergency management agency, and hospital wants priority for homeland security funding. The demand is unlimited, but we must keep the other threats in perspective.

Since 2001, no Americans have died in our homeland from terrorism (as of this writing). During the past three years, 15,000 have died from food poisoning, 120,000 have died from automobile accidents, nearly 300,000 have died from medical mistakes, 1,500,000 have died from cancer, and more than 2,000,000 have died from heart disease.

A nuclear weapon in an American city or an attack with a sophisticated biological weapon could exceed all of these numbers, combined. Either one of these attacks could easily exceed the number of Americans killed in all wars during the past two centuries.

Therefore, our priorities for homeland security spending must focus on preventing terrorists from obtaining weapons-grade nuclear material, building a national system to improve mitigation and response to bioattacks, educating senior government and industry leaders, and exploiting our asymmetric advantage in information systems.

We must avoid misguided efforts that lack a strategic focus, waste scarce resources, and burden American corporations with unsound requirements, lest we become our own worst enemy.

---

1 Dr. Robert Kadlec has worked for two decades in the biodefense field, including assignments in DOD, the CIA, the White House, and Congress.

2 http://www.potomacinstitute.org/research/projectguardian/pgintro.htm/.

Development of Joint Technical Architectures for the Department of Defense

By Sandra J. Freiter, BTAS Inc., 642 ELSS, Hanscom, AFB, MA

The 1996 bombing of the United States Air Force Khobar Towers complex in Saudi Arabia, the 2000 attack on the USS COLE in Yemen, and the 2001 attack on the Pentagon using a hijacked plane are tragic reminders of the threats our military faces each day. And the continued attacks against military installations in Iraq demonstrate that terrorists and insurgents still pose a significant threat to our armed Services. How useful are military technological advances if our bases, buildings, and soldiers cannot be adequately secured and protected? How safe is our military without this protection?

To combat future attacks, the Department of Defense (DOD) is increasing security measures and developing innovative antiterrorism/force protection (AT/FP) equipment.

The question of how the government can better protect its military assets is one that the Physical Security Equipment Action Group (PSEAG) and the Security Equipment Information Working Group (SEIWG), in particular, seek to answer.

The PSEAG is the central manager for all Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E) within the DOD, and SEIWG is one of its standing subcommittees. These groups have been on the forefront of worldwide military security solutions for nearly 20 years. SEIWG's mission is to coordinate and influence system architecture, technical design, and systems integration of all DOD physical security equipment. In support of this DOD-wide effort, SEIWG has a multi-service membership that includes the US Air Force, Army, Navy, and Marine Corps (Figure 1).

Figure 1. Organizational Relationships

The SEIWG chairperson rotates among the four Services approximately every two years; the current chair is Mr. Roy Higgins of the 642d Electronic Systems Squadron at Hanscom Air Force Base in Bedford, Massachusetts.

The US Air Force (USAF) Electronic Systems Center 642d Electronic Systems Squadron (642 ELSS, formerly the Force Protection System Squadron) at Hanscom Air Force Base is supporting the SEIWG in developing a joint PSE technical architecture for application to all DOD PSE design and acquisition efforts. The architecture consists of three "views": the Operational View, the Systems View, and the Technical View

(Figure 2). The Operational View depicts the operational requirements with the elements, tasks, and activities involved in meeting those requirements, as well as information flows required to accomplish operational mission requirements. The Systems View describes and interrelates the existing or postulated system designs, technologies, equipment, and other resources to support the operational requirements. The Technical View describes the profile of rules, standards, and conventions governing systems implementation.

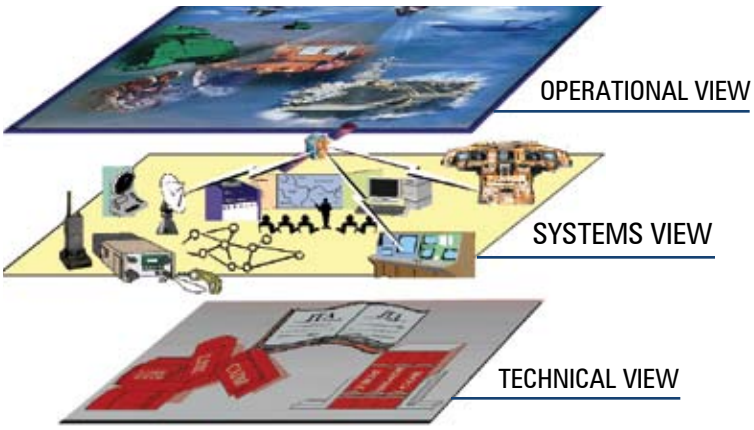


Figure 2. Joint Physical Security Equipment Architecture

In developing a joint PSE architecture embraced by all of the armed Services, the SEIWG's primary vision is of security systems with shortened and less costly acquisition and development phases, minimized RDT&E duplication, increased service interoperability and interchangeability, and easier maintenance. The joint architecture aims to integrate the future DOD security systems across the four military Services and to minimize the need for physical redesigns. This translates into increased protection against international and domestic threats at lower costs and in reduced timeframes.

The SEIWG is accomplishing this ambitious goal through its work across all three of the architectural views. Over the past several years, the SEIWG has focused on the Technical View through the development of the Joint Anti-Terrorism/Force Protection Technical Standards Profile (TV–1) and Interface Control Documents (ICDs) for AT/FP equipment. These Technical View products will be used by all four Services during the acquisition and development of future PSE.

The TV–1 document, currently being prepared under contract to the USAF, is a compilation of AT/FP equipment standards. The document provides a focused profile of standards and protocols currently used by all the Services in the development and procurement of physical security systems, equipment, and components for the 2007–2008 timeframe. This resource allows program managers to identify current, applicable AT/FP standards. A Microsoft Word document provides a brief synopsis of each standard, identifies the relevant areas to which the standard applies, identifies related or companion standards, and provides hyperlinks to the standard or its source. The standards are organized loosely by relevant categories, such as common infrastructure; communication; command, control, and display equipment; access control; detection; surveillance; delay denial response; and power.

Adherence to the TV–1 standards will promote interoperability and commonality at every level of force protection.

To avoid presenting a biased position and possibly influencing system developers and architecture users toward a particular commercial solution, the TV–1 product focuses only on AT/FP-related technologies and the standards that support them and does not discuss the commercial products that implement the standards. But adherence to the TV–1 standards will promote interoperability and commonality at every level of force protection.

Plans are in place to review, update, and reissue the TV–1 document as deemed necessary by the SEIWG. The standards in the TV–1 document will be reviewed against the following criteria:

- Applicable to AT/FP equipment and systems
- Viable relative to industry trends and technology evolution
- Mature and used by at least three vendors in their product offerings
- Provide one or more required components relative to the needs defined in Operational and Systems Views
- Compatible and integrate well with the overall set of selected technology
- Supportive of the directions of DOD systems, such as net-centric, service-oriented, and component-based, and use of the Global Information Grid (GIG)
- Not proprietary.

An effort is currently underway to convert this Microsoft Word document into an easy-to-use database that will be available in 2008 in both a web-based and a stand-alone version. The initial database, with all the information in the current TV–1 document, will facilitate the search for various types of AT/FP-related information and standards, providing a valuable tool for AT/FP program managers.

The TV–1 document, not due out until June 2007, can be obtained via a request through the SEIWG chairman, Mr. Roy Higgins.

The TV–1 effort is just one way that the SEIWG is working to develop a joint PSE technical architecture. The SEIWG is also focusing on generating Interface Control Documents to standardize the communication interface between AT/FP systems using the eXtensible Markup Language (XML) 1.0, as defined by the World Wide Web Consortium. The recently published SEIWG ICD–0100 document defines the structure and sequencing of information for communication between systems using XML. This ICD is broad enough to be applied to a variety of system types although its focus is on AT/FP information exchange. This ICD, being applied by industry today, is available from the SEIWG chairman.

The SEIWG is developing two other specific ICDs. The first describes the communication between a centrally located system known as the Command, Control, and Display Equipment (CCDE) that monitors security alarms and the security situation in a base defense system, the devices causing the alarms, and other information. This ICD consists of a series of sub-ICDs, or tabs, that standardize the XML schemas between the CCDE and AT/FP sensor equipment components. The ICD focuses on the communication interface between the CCDE and the detection, surveillance/assessment, access control, delay/denial, mass notification, and response devices, including remotely operated weapons.

In addition to standardizing the communication in the hierarchal relationship between the CCDE and sensors, the SEIWG is developing a second ICD: the CCDE-to-CCDE ICD. This ICD provides various XML schemas for standardizing CCDE-to-CCDE communication, ensuring that multiple CCDEs can effectively share AT/FP information and that vendor equipment is interoperable. This comprehensive integration provides maximum safety, operational, and situational awareness, and mitigates alarm response costs.

Although much of the SEIWG's work has focused on the Technical View, the SEIWG also produced Operational and System View products with multiservice utility. The SEIWG drafted the High-Level Operational Concept Graphic, known as an OV–1, and the Operational Activity Model, or OV–5. The SEIWG also developed a draft Systems Interface Description, known as a SV–1, and a lexicon for architectural view terminology. These products are currently in use in the four Services' Joint Capabilities Technology Demonstration, which is part of a larger DOD effort to rapidly place relevant, mature technology into the hands of joint and coalition warfighters.

With the maturation of these products over the next year, the SEIWG anticipates that the DOD AT/FP systems for every Service will develop a cohesive architecture consisting of products from many vendors seamlessly exchanging information. Adherence to the AT/FP standards identified in the TV documents—as well as the ICDs—will reduce acquisition and development time, minimize RDT&E, increase Service interoperability and interchangeability, and ease maintenance. All of these factors will increase the safety of our military assets.

MITRE Corporation has established a SEIWG Document Repository on its MITRE Force Protection SEIWG SharePoint web site, which contains all SEIWG-approved industry and DOD documents.

To access the repository, visit the Hanscom Air Force Base Electronic Request for Proposals Bulletin Board (HERBB) at http://www.herbb.hanscom.af.mil and follow the instructions for joining the MITRE Force Protection SEIWG SharePoint website. From the home page, click on "GO" in the "Business Opportunities" area without entering anything, which will bring up an alphabetical list of pages. Scroll down and select the "Security Equipment Integration Working Group (SEIWG) Documents." A brief summary of the SEIWG's mission and instructions for accessing the SharePoint web site will display.

For more information on SEIWG's work or its documents, you may also contact any of the SEIWG representatives listed below.

Editor's note: The TV–1 has been released and is available to DOD and the Physical Security community. It can be obtained via request from the Service representatives or from the Hanscom Air Force Base Electronic Request for Proposals Bulletin Board (HERBB) web site.

Service Representative	Organization	Telephone	E-mail
Mr. Roy Higgins	USAF	(781) 377-4790	roy.higgins@hanscom.af.mil
Mr. Timothy Bootle	USMC	(843) 218-5269	timothy.bootle@navy.mil
Mr. Richard Goehring	USA	(703) 704-2524	richard.goehring@belvoir.army.mil
Mr. Edward Layo	USN	(202) 746-8247	edward.layo@navy.mil

Notes from the War on Terror

Overcoming the ideology of hate and terror

Information collected by the J-5
Strategic Plans and Policy Directorate

"A festering Palestinian problem, among all factors, is the single most important factor perpetuating the tension between the West in general and the Muslim world as a whole … We must accept the fact that the plight of the Palestinians has come to epitomize everything that is unjust and unfair to the treatment of peoples ... The feeling of being humiliated has transformed into hostility."

Malaysian PM Abdullah Ahmad Badawi
Middle East Online
22 May 2007

"For a long time now, al Qaeda's actions have been rather peculiar and they have intensified since the formation of the so-called Dawlat Al-Iraq Al-Islamiya (the Islamic State of Iraq). They have been behaving strangely toward Sunnis and killing those who have not pledged allegiance to them. They attacked mosques in the 'Amiriya area … They are killing [worshippers] in mosques. Why are they targeting Sunnis when the sectarian militias that are supported by Iran are targeting them? We question what the purpose of these actions is."

Ibrahim Shammari
Official Spokesman Islamic Army in Iraq
Al-Jazeera/CIIR
4 June 2007

"What we are suffering from in Iraq … is foreign interference … whether it is coming from the US or not. Yes, the occupation is the founding member of Iraq's ruin. But there are those who come from outside of Iraq … to carry out killings, bombings, and to tear Shiite and Sunni Iraqis apart."

Sheikh Salah Ubaydi
Media Official, Sadr Movement, Najaf
Al-Jazeera/CIIR
29 May 2007

"It is not a setback for us when we lose this man (Taliban commander Mullah Dadullah), since we do not win due to efforts of men: We win when God wants us victorious."

Islamic State of Iraq
Al-Fajr Media Center
BBC
15 May 2007

"It was not America's perceived weakness that brought about the September 11 attacks, as [Prof. Bernard] Lewis argues, but rather its undeniable prowess. This is because Mr. bin Laden and other Islamists' war is not against America per se, but is rather the most recent manifestation of the millenarian jihad for a universal Islamic empire, the umma. As the preeminent world power for quite some time, and the only remaining superpower after the collapse of the Soviet empire, America blocks the final realization of this goal and hence is a natural target for aggression. In this sense, the House of Islam's war for world mastery is a traditional, indeed venerable, quest that is far from over."

Dr. Efraim Karsh
University of London
New York Sun
18 May 2007

"The jihad in Iraq today… is moving from the stage of defeat of the Crusader invaders and their traitorous underlings to the stage of consolidating a Mujahid Islamic Emirate which will liberate the homelands of Islam, protect the sacred things of the Muslims, implement the rules of the Sharia, give the weak and oppressed their rights back, and raise the banner of jihad as it makes its way through a rugged path of sacrifice and giving towards the environs of Jerusalem."

Ayman al-Zawahiri
AQ No. 2
Jihadist Websites/OCR
5 May 2007

"I am issuing a firm warning. If the Palestinian people have no way out, and if the siege, the collective sanctions, Israeli aggression and the absence of a political perspective continue ... this will lead to a big explosion that will not only affect the Palestinians but the entire region, notably the Zionist entity … In my opinion, today's conditions resemble those in the late 1990s ... that prepared the ground for the intifada."

Khaled Meshaal
Hamas Political chief
Middle East Online
30 April 2007

Notes from the War on Terror

Current events and their effect on the Global Antiterrorist Environment (GATE)

Information collected by the J-5 Strategic Plans and Policy Directorate

Negative effects on the GATE

Event	Strategic Significance
Iraq: New Attack on Golden Mosque. Iraqi Shia leaders appealed for calm after another terrorist attack on the al-Askari shrine in Samarra destroyed the damaged building's two minarets.	The shrine, one of the holiest sites of Shia Islam, is believed to contain the remains of the 10th and 11th imams. The February 2006 bombing of the dome greatly intensified sectarian violence in Iraq. The perpetrators of the latest desecration are intolerant extremists who want to prevent national reconciliation by triggering more Sunni–Shia violence.
Iraq/Iran: Iran's Summer Strategy. Iran is secretly forging ties with al Qaeda elements and Sunni Arab militias in Iraq in preparation for a summer showdown with coalition forces intended to tip a wavering US Congress into voting for full military withdrawal, according to an article (quoting unnamed US officials) in the left-leaning Guardian (UK) on 22 May. Syria was described as still collaborating closely with Iran's strategy in Iraq, serving as a conduit for most foreign fighters. Iran was also said to be supporting and supplying the Taliban in Afghanistan against Coalition forces.	In this view, the Iranian government, despite entering into discussions with the US and regional states on Iraq, is increasingly confident of its domestic and international position and is willing to risk escalating its support for those trying to drive coalition forces from Iraq and Afghanistan.
Al Qaeda: "Legitimate Demands." AQ spokesman and US citizen Adam Yahiya Gadahn presented his organization's non-negotiable demands to the US government in a video speech produced by AQ's as-Shad media arm (SITE Institute, 29 May 2007). His demands are as follows: (1) remove American military forces from Muslim lands, (2) cease encroachment into the political, social, and economic affairs in these countries, and (3) free Muslim captives from prisons. Should these demands not be met, Gadahn stated, "… you and your people will—Allah willing—experience things which will make you forget all about the horrors of September 11th, Afghanistan, Iraq, and Virginia Tech."	Gadahn's diatribe suggests that, in case anyone was wondering, US withdrawal from Iraq would not be nearly enough to reduce global hostilities with al Qaeda. AQ and other violent extremists would proclaim victory and then attempt to bring pressure on additional countries.

Positive effects on the GATE

Event	Strategic Significance
Lebanon: Army Battles Islamist Militants. The Lebanese Army fought with a radical Islamist group based in a Palestinian refugee camp, Nahr al-Bared, in northern Lebanon.	The Fatah Al-Islam group, which includes Palestinians as well as foreign fighters, is reportedly linked to al Qaeda and Syrian intelligence, and its leader had ties to Abu Musab al-Zarqawi. The violent exchange suggests AQ-linked or -inspired terrorist groups may try to expand their influence in areas closer to key targets: Israel and Eqypt.
Pakistan: Government Asks North Waziristan Tribesmen to Expel Taliban and al Qaeda. A government administrator, claiming to be speaking for President Musharraf and the North West Frontier Province governor, asked a meeting of 500 tribesmen and Muslim clerics in Miranshah to expel Taliban and al Qaeda fighters and their supporters from North Waziristan, according to Agence France-Press (AFP).	Since signing controversial agreements with tribesmen in the Waziristans, the government has done very little to rein in the Taliban and AQ in the Afghan border areas. The administrator's reported suggestion would have little direct impact, but could be a welcome sign of some Pakistan government pressure on tribesmen to isolate the Taliban and AQ.
US: National Strategy for Public Diplomacy (PD) and Strategic Communication (SC). The new national strategy contains three strategic objectives: (1) Offering a positive vision of hope and opportunity rooted in basic US values. (2) With US partners, isolating and marginalizing violent extremists who threaten the freedom and peace sought by civilized people of every nation, culture, and faith. (This includes promoting democratization and good governance as a path to a positive future, in secure and pluralistic societies; actively engaging Muslim communities and amplifying mainstream Muslim voices; isolating and discrediting terrorist leaders, facilitators, and organizations; delegitimizing terror as an acceptable tactic to achieve political ends; and demonstrating that the West is open to all religions and not in conflict with any faith.) (3) Nurturing common interests and values between Americans and peoples of different countries, cultures, and faiths across the world. The strategy will address mass audiences, key influencers, and vulnerable populations (youth, women and girls, and minorities). Major PD priorities include expanding education and exchange programs, modernizing communications, and promoting US "diplomacy of deeds" (e.g., health care, education, economic opportunity, food and shelter, training for political participation, disaster relief). Interagency PD and SC coordination will be improved by establishing the Counterterrorism Communications Center at the Department of State to develop messages and strategies to discredit terrorists and their ideology and by designating an interagency crisis communications team.	The long-awaited national strategy aims, among other things, to revitalize US strategic communication efforts to counter violent extremist ideology.

DD AT/HD
Joint Staff, J-3 Operations Directorate
Pentagon
Room MB917
Washington, DC 20318-3000